Department for
Business, Energy
& Industrial Strategy

Office for Product
Safety & Standards

The use of distributed ledgers to verify the provenance of goods

Final Report

BEIS Research Paper Number 2020/036

September 2020

The use of distributed ledgers to verify the provenance of goods

A report for the Office for Product Safety and Standards (OPSS) by London Economics

Acknowledgements

This independent research report was produced by London Economics.

The views expressed in this report are those of the authors, not necessarily those of the Office for Product Safety and Standards or the Department for Business, Energy & Industrial Strategy (nor do they reflect Government policy).

The following organisations were consulted as part of this project. In the interest of data protection, the names of individual respondents from each organisation have been withheld.

- Ambrosus
- Bext360
- Blockchain Labs for Open Collaboration (BLOC)
- Cambridge Centre for Alternative Finance, University of Cambridge
- Circulor
- Enterprise Ethereum Alliance (EEA)
- Everledger
- Food Standards Agency
- Hyperledger
- IBM
- Ministry of Infrastructure and Water Management
- Modum.io
- PegaSys
- SAP
- TE-FOOD
- Omnitude
- Ujo Music
- Verisart
- ConsenSys
- Waltonchain

We are grateful to all respondents for their time and insights.

Any enquiries regarding this publication should be sent to us at:
enquiries@beis.gov.uk

Contents

Executive summary 6
1 Introduction 9
2 Types of distributed ledger technologies 10
2.1 Overview 10
2.1.1 Properties of distributed ledgers 10
2.1.2 Types of distributed ledgers 11
2.2 Blockchain technology 12
2.2.1 Types of blockchain 12
2.2.2 How does blockchain technology work? 13
2.2.3 Relative strengths and weaknesses of different types of blockchain 16
2.2.4 Choosing a type of blockchain 18
2.3 Other types of distributed ledger technologies 18
3 Benefits and challenges of blockchain technology in tracking consumer products 20
3.1 Benefits of blockchain in supply chain management 20
3.1.1 Current challenges faced by the supply chain industry 20
3.1.2 The transformative potential of blockchain 21
3.1.3 Adoption of blockchain-based solutions 23
3.2 Challenges for industrial applications of blockchain 25
3.2.1 Low awareness and understanding 25
3.2.2 Damaged reputation of cryptocurrencies 25
3.2.3 Implementation costs 26
3.2.4 Regulatory uncertainty 26
3.2.5 Lack of interoperability and security vulnerabilities 27
3.2.6 Resistance from parties that benefit from opacity 28
3.2.7 Data quality and integrity 28
3.3 Applications of blockchain in tracking consumer products 29
3.4 Conclusion 31
References 33
4 Appendix 1: Other consensus mechanisms 40
5 Appendix 2: Study methodology 42
5.1 Stage 1: Secondary research 42
5.2 Stage 2: Primary research 43
6 Appendix 3: Applications of blockchain technology in tracking consumer products 44
6.1 Counterfeit prevention 44

6.1.1 Current situation and problems 44
6.1.2 Solutions offered by blockchain 44
6.1.3 Specific application(s) 45
6.1.4 Risks and challenges 47
6.2 Ethical and ecological sourcing 47
6.2.1 Current situation and problems 47
6.2.2 Solutions offered by blockchain 47
6.2.3 Specific application(s) 48
6.2.4 Risks and challenges 51
6.3 Intellectual property protection 51
6.3.1 Current situation and problems 51
6.3.2 Solutions offered by blockchain 52
6.3.3 Specific application(s) 53
6.3.4 Risks and challenges 55
6.4 Environmental control in pharmaceutical cold chains 56
6.4.1 Current situation and problems 56
6.4.2 Solutions offered by blockchain 57
6.4.3 Specific application(s) 58
6.4.4 Risks and challenges 60
6.5 Food safety and standards 60
6.5.1 Current situation and problems 60
6.5.2 Solutions offered by blockchain 62
6.5.3 Specific application(s) 63
6.5.4 Risks and challenges 68

Executive summary

The need to assure the provenance of consumer products

Over the last several decades, globalisation has led to unprecedented complexity in global supply chains, which has aggravated concerns about disruptions, delays, inefficiencies, or fraud. Consequently:

- Businesses face new challenges of maintaining visibility into the origin, authenticity, and handling of products.
- Regulators are facing new challenges in enforcing compliance with standards and protecting public health and safety.
- Consumers are becoming increasingly concerned about ethical or ecological practices in production.

This has led to increasing interest in distributed ledger technology as a means of assuring the provenance of products. In their simplest form, distributed ledgers are digital databases storing information (such as records of transactions, documents, identities and assets) that is shared with all authorised entities in a network. These distributed ledgers are based on various platforms, of which the most well-known is currently blockchain.[1]

Blockchain technology is a specific architecture of a distributed ledger that was first trialled in the financial sector.[2] The first application of blockchain was for the Bitcoin cryptocurrency, but it is its application in supply chains that is showing particular promise.[3]

While blockchain technology offers potential solutions to the challenges facing the supply chain industry, there are a number of risks and challenges along its path to full-scale adoption displayed below in Table 1.

Table 1: Benefits and challenges of blockchain technology in tracing consumer products

Potential benefits	Challenges to adoption
Increased trust, transparency, and accountability between disparate entities in complex supply chains	Low awareness and understanding of the potential of the technology
Process automation through smart contracts	Implementation costs can deter firms, especially when the business value in multi-party networks is unclear
Real-time tracking and monitoring of products	Disruption of existing processes and practices, especially in highly optimised supply chains
Immutable audit trails, full transaction history	Damaged reputation of cryptocurrencies created caution about solutions relying on crypto assets

[1] ABI Research (2017a). “Blockchain Applications: Beyond Fintech to the IoT”. ABI Research Report. Q2 2017.
[2] ABI Research (2017a).
[3] Higginson et al. (2019). “Blockchain’s Occam problem”. McKinsey & Company Article. Published January 2019.

Proof of certification, identity, authenticity or compliance	Some applications may face regulatory uncertainty
Unique, shared source of truth; no data silos but also no central point of failure	Lack of interoperability between different distributed ledger technology implementations
Ultimately, improved product safety and standards	Potential security vulnerabilities in the underlying code or cryptography

At present, blockchain-based solutions are a nascent market and most industrial applications of the technology in supply chain management are in proof-of-concept, prototype, or pilot stage, with a few exceptions in live production.

Types of distributed ledger technologies

A digital distributed ledger has two key properties that distinguish it from traditional centralised ledgers:

- A **decentralised architecture** – Information on a distributed ledger is stored and shared with all authorised entities in a network such that each entity holds an identical copy of the information, which is simultaneously updated when new information is added to the ledger. Specific protocols (called 'consensus mechanisms') ensure that all entities are synchronised with each other and agree on which information is legitimate and added to the ledger.
- **Cryptography** - A mathematical method of concealing and revealing information, which ensures information is only viewable by the intended recipient(s), increasing security and reducing the need for trust amongst entities in the network.

Taken together, these properties provide a transparent, autonomous and immutable system of recording and sharing information. Three different types of distributed ledgers have been developed according to access and validation rights:

1. **Public, permissionless** – Anyone can participate and validate information added to the ledger.
2. **Private, permissioned** – Participation is limited to a closed group of participants who share common interests.
3. **Public, permissioned** – Participation is open to everyone but the ability to share and validate information is limited to one or a selected trusted group of participants.

The relative strengths and weaknesses of the different types of blockchain technology depend on its intended use. Public, permissionless blockchains are best suited for situations where absolute transparency is of value (e.g. records of intellectual property ownership), speed is less critical, and the tools and stack (application logic) of the public protocol are sufficient. Permissioned ledgers are preferable in applications where anonymity is not desirable, some transaction privacy is required, speed is important, and personalisation of the rules of the ledger is needed.

The future of digital, distributed ledgers for assuring the provenance of the supply chain for consumer products

As a cryptographically secured, shared data layer, blockchain technology has the potential to help build trust, transparency, and accountability between disparate entities.

These properties mean that for many consumer products, permissioned ledgers shared amongst companies in the supply chain are ideal for tracing the provenance of a product and have been shown to work well in a wide range of demonstrator projects.

In some established supply chains, many of the benefits of distributed ledgers can be realised by the optimisation of existing methods for assuring provenance. For example, in the pharmaceuticals sector, and some parts of the food sector, a reluctance to change what are already well proven and optimised supply chain documentation systems is likely to slow adoption of these technologies.

Moreover, distributed ledgers are only as good as the quality of their data. Blockchain technology alone does not solve the problem of detecting incorrect inputs. However, in combination with other technologies such as secured seals, tags and sensor technologies, it may reduce the risks arising from such challenges in the supply chain domain.

1 Introduction

Distributed ledger technologies offer a unique combination of characteristics that could make them an attractive method for assuring the provenance of consumer products.

These include:

- **Transparency and Immutability** – Multiple copies of all records are accessible to all authorised entities and remain tamper-proof and auditable, which makes information more reliable at each stage of the supply chain and allows for end-to-end visibility.
- **Trust and Security** – Given the distributed nature of the technology as well as advanced encryption and validation processes, there is growing level of trust in information along the supply chain, which also adds value.
- **Efficiency and Innovation** – With no intermediary, transactions can be settled faster and at a lower cost. Moreover, new business models are being developed to benefit from potential efficiency gains.

First used to support the Bitcoin cryptocurrency, distributed ledger technologies, such as blockchain, are now attracting interest from business supply chains, regulators and consumers in other sectors. This includes industries such as food and agriculture, healthcare and pharmaceuticals, creative arts, as well as markets for high-value luxury goods.

However, the use of distributed ledgers is still at an early stage, and it is not clear what the practical issues will be when used in the supply chains of different types of consumer products

The objective of this report is therefore to critically assess the use of distributed ledgers in sectors where they have already been trialled, developing an evidence base to help inform their use in the supply chains for different types of consumer product.

The detailed research programme comprised desk research followed by industry interviews (Appendix 3: Applications of blockchain technology in tracking consumer products). It addresses two primary questions:

- Distinguish between the different types of distributed ledger technologies, how they work (in the context of the blockchain technology) and their relative strengths and weaknesses.
- Review where these technologies are being used (or piloted for use) to verify the provenance of consumer products or of the components used in the supply chain of these consumer products, identifying success factors as well as potential opportunities and challenges faced.

2 Types of distributed ledger technologies

Distributed ledgers use a variety of technology platforms, of which blockchain is perhaps the most well-known.[4] An early use of the blockchain platform was to support the Bitcoin[5] cryptocurrency, since when iterations of the technology have been developed to suit other business application requirements.[6] With ongoing development, terminology in the field has yet to be fully formalised and hence, terms such as blockchain, distributed ledgers and shared ledgers are often used interchangeably.[7] For clarity, 'distributed ledger technologies' is used as an umbrella term to describe the various types of the technology,[8] with the focus of this report being on the different types of blockchain and their application.

This chapter is split into three sections:

- An overview of the properties of different types of distributed ledgers, categorising them based on accessibility and validation.
- The emergence of the blockchain technology, describing how it works and assessing the relative strengths and weaknesses of its different types.
- Other forms of distributed ledger technologies.

2.1 Overview

2.1.1 Properties of distributed ledgers

A distributed ledger is a digital database with two key properties that distinguish it from traditional centralised ledgers:[9]

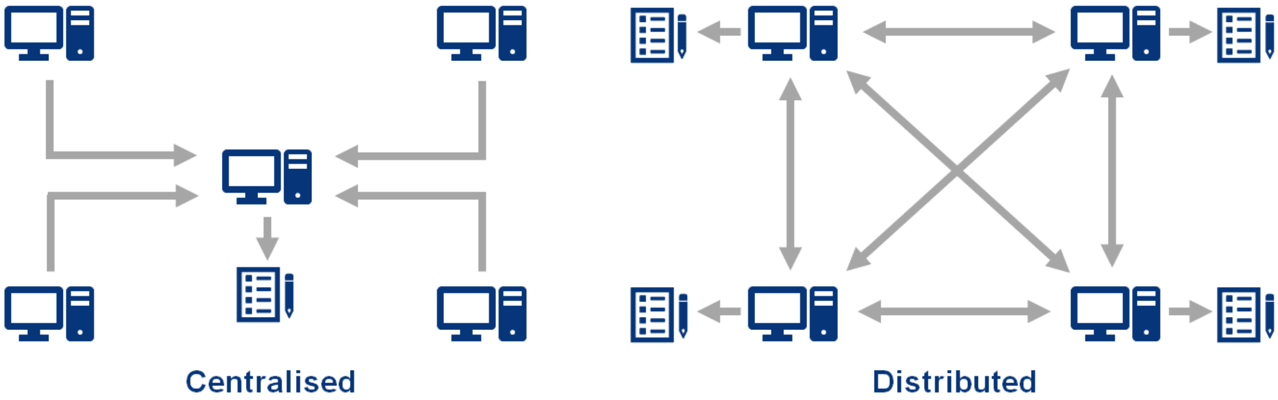
- Information is stored and shared with all authorised entities in a network such that each entity holds an identical copy of the information. Each copy of the ledger is simultaneously updated when new information is added. This **decentralised architecture** (Figure 1) eliminates the need for a central authority or intermediary to pass information to each entity.
- Information is secured using **cryptography**, which is a mathematical method of concealing and revealing information. This ensures that information is only viewable by the intended recipient(s), and also eliminates the need for trust amongst entities in the network. The information seen by each participant is synchronised, and all entities must agree on which information is legitimate before it is added to the ledger.

---

[4] ABI Research (2017a).
[5] Nakamoto (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System".
[6] Bogart and Rice (2015).
[7] For example, see UK Government Office for Science (2016), World Bank Group (2017) and Deshpande et al. (2017).
[8] World Bank Group (2017).
[9] Deshpande et al (2017). 'Understanding the landscape of Distributed Ledger Technologies/Blockchain'. RAND Europe. Research study funded by the British Standards Institution.

Taken together, these properties provide a transparent, autonomous and immutable system of recording and sharing information. Section 2.2.1 provides a more detailed discussion on how these two properties are achieved in practice for the blockchain technology.

Figure 1 Centralised versus distributed ledgers



Source: London Economics

1.1.1 Types of distributed ledgers

In general, the different types of distributed ledgers can be classified using two criteria:

- Who has **access** to the distributed ledger? Participation in a distributed ledger may be open to everyone (i.e. public) or limited to a closed group of participants in a network (i.e. private).[10]
- Who has **permission** to validate information added to the distributed ledger? A distributed ledger is permissionless if anyone can contribute and validate information that enters the ledger. In contrast, a distributed ledger is categorised as permissioned if verification of information is determined by one or a group of trusted participants.[11]

Based on these features, three specific types of distributed ledgers have been developed:

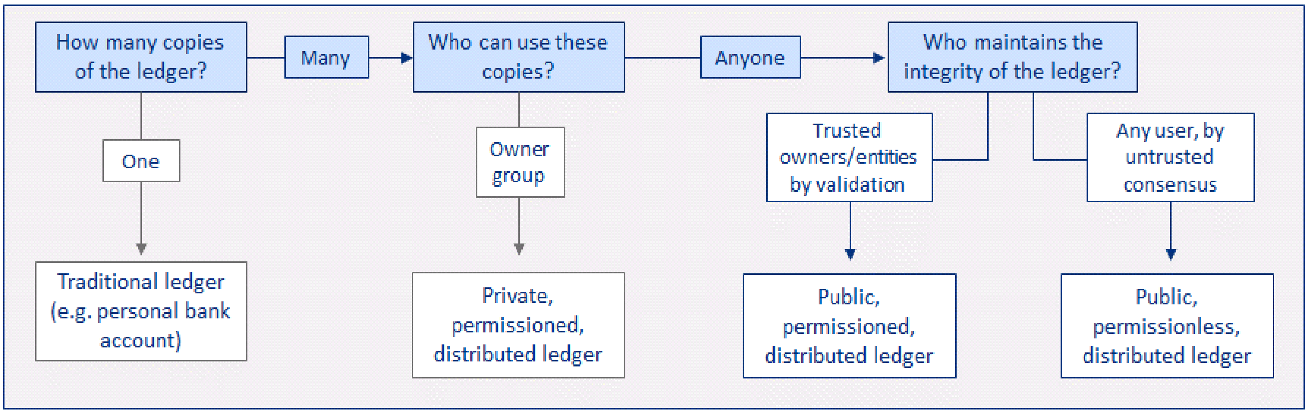
- **Public, permissionless** – Anyone can participate and validate information added to the ledger.
- **Private, permissioned** – Participation is limited to a closed group of participants who share common interests.
- **Public, permissioned** – Participation is open to everyone, but the ability to share and validate information is limited to one or a selected trusted group of participants.

Figure 2 below provides a classification system for the different types of distributed ledger technologies.

Blockchain technology is a specific architecture of a distributed ledger and widely recognised as an emerging technology that has the potential to transform established industries.[12]

[10] Benos, Garratt, and Gurrola-Perez (2017). "The economics of distributed ledger technology for securities settlement". Bank of England. Staff Working Paper No. 670.
[11] Benos, Garratt, and Gurrola-Perez (2017).
[12] ABI Research, 2017a.

Figure 2: Classification of distributed ledger technologies



Source: UK Government Office for Science (2016) (Consult Hyperion). Recreated by London Economics.

1.2 Blockchain technology

1.2.1 Types of blockchain

In 2008, a pseudonymous person (or group of people) named Satoshi Nakamoto published a paper titled ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, that proposed an open, real-time, peer-to-peer payments system, **Bitcoin**, which did not require a centralised trusted authority. This conceptual breakthrough led to a rapid rise in digital currency systems;[13] with the supporting distributed ledger technology now being considered for applications beyond digital currency payments.[14]

Bitcoin is an example of a decentralised peer-to-peer payments system that does not have any owner, and anyone can make contributions to the ledger, and so is an example of a public, permissionless distributed ledger. Since its release in January 2007, alternative types of blockchain have emerged which combine elements of centralised and decentralised infrastructures to suit specific applications. Examples include:

- **Ripple** is a global financial transactions system used for real-time settlement, currency exchange and remittance, which selects a group of participants (known as ‘Unique Node Validators’) from a list of pre-identified set of trusted validators to ensure consistency and integrity of the ledger.[15] This is an example of a public, permissioned distributed ledger.

- **Ethereum** is an open software platform based on blockchain technology that enables developers to build and deploy decentralised applications (referred to as ‘dApps’), which allow developers to build software applications on top of the blockchain layer. One such application is a smart contract, which was initially proposed by Szabo in 1996.[16]

  In this instance, the underlying distributed ledger is public and permissionless.

[13] The price of a Bitcoin has increased by approximately 420% in the period from January 2014 to February 2019. At the time of reporting, its market capitalisation is approximately $66 billion (Thomson Reuters) and the total market capitalisation of cryptocurrencies is estimated to be $122 billion (CoinMarketCap).
[14] Bogart and Rice (2015).
[15] XRP Ledger Documentation. Available here: https://developers.ripple.com/docs.html. [Accessed on 11/10/2018]
[16] Szabo (1996). ‘Smart Contracts: Building Blocks for Digital Markets’.

Smart contracts use computational code to execute a specified action or set of actions when certain conditions have been fulfilled. There are potential benefits of smart contracts such as instant implementation and lower costs of contracting, enforcement and compliance, as well as potential risks such as legal enforceability and dependence on a computing system to execute the correct actions.[17]

- The **R3 consortium** is a joint platform for global financial institutions, initially dedicated to the research of blockchain technology. The resulting open-source network called Corda is a private, permissioned distributed ledger used by the participating financial institutions.[18]

- **BigChainDB** combines blockchain technology with a distributed database. The distributed ledger is permissioned but can support either public or private implementation. The blockchain layer with permissioned validators should secure immutability of data, while the distributed database enables scale and can be queried.[19]

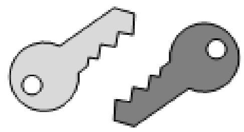
1.2.2 How does blockchain technology work?

A blockchain consists of a number of data units, or ‘blocks’, in which information is recorded and aggregated. New blocks are added to the existing blocks of information to form an append-only database, or ‘chain’. As developed by Nakamoto in 2008, blockchain combines three technologies to achieve a tamper-proof distributed ledger; namely, **digital signatures**, **hashing** and a **consensus mechanism**.[20] A simple step-by-step illustration of how blockchain (in the case of Bitcoin) integrates these technologies is shown in Figure 3.

Figure 3: How blockchain technology works

1 Participant A wants to send information to Participant B (e.g. make a payment in Bitcoin)

2 In order to do this, Participant A requires their private key and Participant B’s public key.



Digital signatures and hashing

Both digital signatures and hashing are cryptographic concepts. Given anonymity in a permissionless blockchain, individuals need to verify their identity in order to execute a transaction (e.g. a payment by cryptocurrency, an exchange or update of a record or other information). This is achieved using asymmetric cryptography.

Each participant in the network is given a pair of keys; a public and private key. Together, these form a digital signature which verifies the participant. The relationship between the

[17] UK Government Office for Science (2016). ‘Distributed ledger technology: beyond block chain’. A report by the UK Government Chief Scientific Adviser.
[18] ABI Research (2017a).
[19] BigChainDB (2016). ‘What is BigChainDB?’. Blog post. 14 February 2016.
[20] ABI Research (2017a).

public and private key is one-way (i.e. asymmetric) such that the public key can be derived from the private key, but the private key cannot be derived from the public. Such a relationship is built using a cryptographic hash function which takes a given input and generates a unique output, from which the input cannot be recreated. Therefore, when a participant wants to make a transaction, they sign the transaction using their private key and other participants verify this signature with the participant's public key.

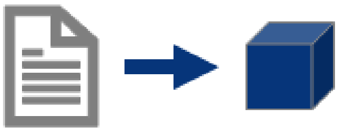
A cryptographic hash function is also used to maintain the immutability of the blockchain. Each block contains:

1) A header containing various metadata about the block, e.g., the version of the block and a timestamp; and,

2) The main body of the block contains the relevant information (e.g. a set of transactions). Within the block header, there is a cryptographic hash of the previous block in the chain.

The hash makes the blockchain secure as asymmetric cryptographic links between individual blocks mean that retrospective changes to information requires updating the block itself as well as all other blocks following this block in the chain.

3 Once Participant A retrieves Participant B's public key, this information is added to a new block along with all other transactions at that time.



4 Given the distributed nature of network, all 'miners' in the network are informed of the impending transaction.

5 Miners compete to solve a complex cryptographic puzzle, which requires intensive computing power. This is known as the consensus mechanism.

Consensus mechanism

The decentralised architecture of blockchain requires some governance principles that decide how new information can be added into the distributed ledger. A consensus mechanism is a way in which the nodes (i.e. participants) in the blockchain network agree on the state of the blockchain. When changes to the blockchain are made, for example a new block is added, the nodes within a network have to agree on the changes before the changes are added to the blockchain. Whether a change is accepted or not depends on whether it complies with a number of rules, often referred to as the consensus rules.

The type of consensus mechanism used depends on who is allowed to validate new information entering the distributed ledger.

Given the lack of restrictions on participation, permissionless blockchains can have thousands of participants (or 'nodes'). Moreover, most public blockchains permit anonymity.[21] Therefore, the governance systems of such blockchains cannot rely on trust between participants. Instead, permissionless blockchains make use of game theory in the design of crypto-economic incentives that motivate participants to maintain the integrity of the ledger.[22]

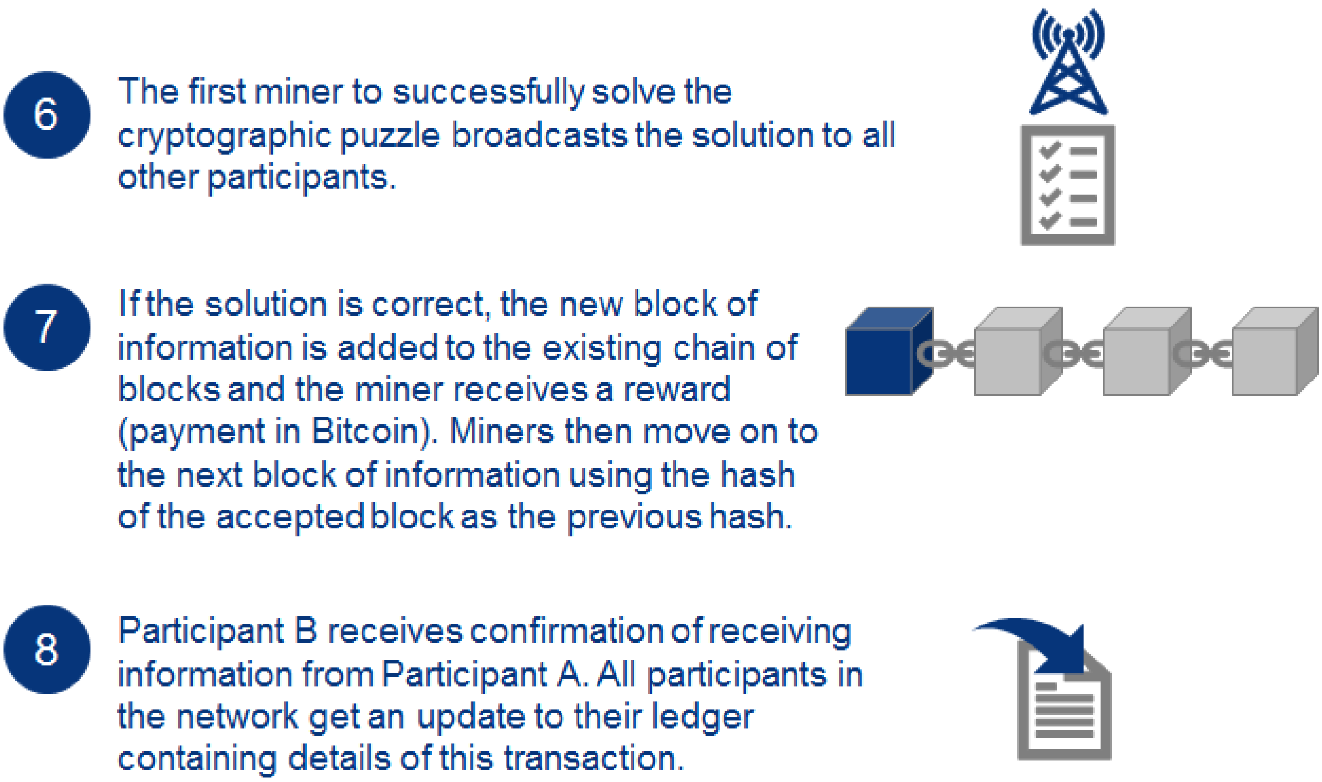
For example, Bitcoin uses the **Proof-of-Work** (PoW) protocol to reach consensus.[23] In this instance, participants in the blockchain network known as 'miners' must solve a computationally-intensive (in terms of computing power and processing time) cryptographic puzzle to validate changes to the blockchain.[24] It is assumed that miners are rational economic actors and consider the trade-off between the high costs (in time and money) incurred to run mining computers and the reward of solving the puzzle (which in the case of Bitcoin is the digital currency itself).[25]

The development of different types of blockchains has also led to alternative crypto-economic incentive designs to address specific issues (such as level of security, extent of decentralisation, and resource efficiency). A detailed discussion on these is provided in Appendix 1: Other consensus mechanisms.

In theory, permissioned blockchains can have any rules. The blockchain is controlled by a finite group of known participants, who often are able to maintain some trust in each other's conduct.[26] Permissioned blockchains used by a small group of participants do not use crypto-economic incentives to maintain the integrity of the ledger. However, this does not mean that the data is necessarily less reliable in comparison to public, permissionless ledgers. The private network can still enforce transactional rules that help ensure proper accounting and resistance to errors or fraud by individual users/systems.[27]

In both permissioned and permissionless blockchains, data immutability does not arise from the technology itself but rather the incentives it creates. In the above example of a PoW permissionless protocol, the network integrity is protected by the prohibitive cost of collecting sufficient computing power to dominate the distributed network. In permissioned blockchains, the transactional rules are pre-defined by the identified network participants who have existing commercial and legal relationships. Any potential malpractice is visible in the cryptographic audit trail, deterring any wrongdoing.

[21] Voshmgir and Kalinov (2017). 'Blockchain Handbook: A Beginners Guide'.
[22] Voshmgir and Kalinov (2017).
[23] Nakamoto (2008).
[24] World Bank Group (2017). 'Distributed Ledger Technology (DLT) and Blockchain'. FinTech Note Number 1.
[25] Brennan and Lunn (2016).
[26] Brennan and Lunn (2016).
[27] He3 Labs (2018). 'Hybrid Blockchain Solutions: Real-World Combinations of Public and Private Distributed Ledger Technology (DLT)'. Blog post. 23 July 2018.



Source: London Economics

1.2.3 Relative strengths and weaknesses of different types of blockchain

The relative strengths and weaknesses of the different types of blockchain technology depends on its intended use. Table 2 summarises key trade-offs in terms of security, speed, scalability, flexibility and resource efficiency.

Table 2: Strengths and weaknesses of different types of blockchain

Feature	Permissionless blockchain	Permissioned blockchain
Accessibility	Public	Public or Private
Security and integrity	**+** 'Trustless': The trustworthiness of the data is built into the system. The combination of cryptography and a consensus mechanism that shapes economic incentives can make the system immune to malicious or fraudulent behaviour. **-** The network design makes it costly but not impossible to compromise the integrity of the ledger. For example, if an individual or organisation acquires 51% of the mining power (known as the 'hashrate') of all nodes, they could gain control of the network and decide which information gets approved and which not, or even alter recently added information.	**+** Individual participants are identified, and all changes to the ledger are recorded in the cryptographic audit trail. Such transparency and accountability disincentivises malpractice. **+** With an appropriate consensus mechanism, no single entity controls the data and the governance rules ensure resistance to errors/fraud by individual participants. **-** Given the small number of participants and customisable governance rules, one or more parties can become dominant. The decentralised architecture itself does not guarantee integrity of the ledger.
Speed and scalability	**-** Time-consuming as the number of transactions increases. Moreover, as	**+** Fast and scalable given a smaller number of identifiable participants with defined roles and

	there is a limit on the size of a block, transactions may be stuck in a queue before they can be processed. Bitcoin currently processes 61 transactions per second on average, with one block being added to the chain approximately every ten minutes.[28] In contrast, Visa can process more than 24,000 transactions per second (Based on testing conducted with IBM in 2010).	a computationally simpler consensus mechanism.
Flexibility and adjustability	**+** Although developers cannot change the core blockchain layer, some blockchain protocols (e.g. Ethereum) allow personalisation of the layers on top of the core blockchain (e.g. decentralised applications) **-** Cannot be changed or adjusted to suit a particular business use. The only way to change the implementation of the network is a so called 'hard fork', where a change in the underlying code essentially means creating a new blockchain network that operates by the new rules. Bitcoin, for example, has already experienced such a split, which created Bitcoin Cash. Similarly, Ethereum has a twin called Ethereum Classic.	**+** Offers far greater flexibility as software developers can personalise both the blockchain layer and any other applications built on top of it. If the group of network participants agree, they can relatively easily modify and adjust a blockchain network to suit their business needs. For example, Hyperledger, a multi-project business collaboration hosted by the Linux Foundation, provides several open source blockchain implementations that businesses can use and personalise.
Resource efficiency	**+** Alternative consensus mechanisms for permissionless blockchains have been designed which have a reduced cost/more efficient infrastructure. However, these alternative mechanisms typically come at the cost of reduced security or decentralisation. Some examples are discussed in more detail in Appendix 1. **-** Accessible by everyone so the blockchain can become very long. Moreover, the Proof-of-Work consensus mechanism means that miners effectively compete against each other to solve cryptographic puzzles; thus, a lot of processing power is used to perform the same task and a significant cost incurred. For example, Bitcoin's current electricity consumption is estimated to be approximately 73 TWh per year, which is similar to that of countries such as Austria (72 TWh), Chile (72 TWh) or the Czech Republic (67 TWh).[29]	**+** Parties sharing a permissioned blockchain can agree on any kind of consensus mechanism. Some common structures for public permissioned blockchains are reviewed in Appendix 1.

Sources: World Bank Group (2017), Bogart and Rice (2015), Deloitte (2017b), Brennan and Lunn (2016), Brennan et al. (2018) and Deshpande et al. (2016).

[28] Coinanalysis (2018). 'How many transactions per second can Bitcoin Cash handle?'.
[29] Digiconomist (2018). 'Bitcoin Energy Consumption Index'.

1.2.4 Choosing a type of blockchain

The choice of a suitable blockchain implementation depends on the purpose of the network. Public, permissionless blockchains are optimal in situations where absolute transparency is of value (e.g. records of ownership), speed is of lower importance, and the tools and stack (application logic) of the public protocol are sufficient. An appropriate crypto-economic incentive mechanism (e.g. Proof-of-Work) should be used that best matches the desired balance between scalability, security, and decentralisation.

Permissionless blockchains also protect users of decentralised applications (dApps) from their developers. Even the creators of the apps cannot change the underlying blockchain layer, and therefore cannot control the transactions in the app. Finally, permissionless blockchains can benefit from network effects. Since anyone can participate in the network, permissionless blockchains may be more suitable for products that aspire for mass-market reach. However, this is dependent on the choice of the consensus mechanism which determines the operational performance and ability of the distributed ledger to scalability.[30] This dispersion of power and economic incentive systems that safeguard data integrity make public permissionless blockchains more technologically radical and disruptive than their permissioned counterparts, which entail a greater level of centralisation and require more trust among participants.

Permissioned ledgers are preferable in applications where anonymity is not desirable, some transaction privacy is required, speed is important, and personalisation of the rules of the ledger is needed. The technological innovation of permissioned ledgers is arguably less profound, but this can also make them more readily applicable.

1.3 Other types of distributed ledger technologies

As mentioned above, there is an increasing number of variations in the blockchain technology, as well as innovations that build upon blockchain or are inspired by blockchain. Since 2009, more than 8,600 new projects were started on average every year, with almost 27,000 in 2016 alone (Deloitte, 2017a). Of the total estimated 86,000 blockchain projects developed by 2017, 89% were created by individuals and 11% by organisations. However, only 8% of these projects are still actively maintained, shortening the average life span of a project to 1.22 years (Deloitte, 2017a). This has led to the emergence of ‘distributed ledger technologies’ as an umbrella term. Table 3 provides some examples of the types of distributed ledger technologies that have been developed since the introduction of blockchain.

Table 3: Other types of distributed ledger technologies

Distributed ledger technology	Description
Tangle	Tangle introduces a transaction storing mechanism that is structured in groups of data nodes rather than blocks. Its miner-free validation process is far more agile than public blockchains, but arguably less secure.[31] The technology is designed for supporting large number of interconnected devices in the so called Internet-of-Things, and is most closely associated with Tangle’s cryptocurrency, IOTA.

[30] Deloitte (2016). ‘Blockchain: Enigma. Paradox. Opportunity’. Deloitte LLP.
[31] IG (2018). ‘The tangle vs blockchain: A comparison between IOTA and bitcoin’. Published on 9 July 2018.

Hedera Hashgraph	Hedera Hashgraph also tries to address blockchain's problems with speed. It introduces a different form of distributed consensus based on virtual voting using rapid communication between nodes known as 'gossip' and 'gossip about gossip' protocols. According to the developers, the system also facilitates more security, avoiding blockchain's susceptibility to '51% attacks'.
Holochain	Holochain uses a simpler, faster and cheaper architecture than permissionless blockchains to power decentralised peer-to-peer applications. Each device has its own secure ledger and data are synchronised only as agreed by users, preventing any sharing or sale of data to third parties by network providers. Examples of intended uses include social networks, collaboration tools, or sharing economy apps.
Nano Block Lattice	Nano's mission is to a develop a leading cryptocurrency with split-second transactions. Like other alternatives to blockchain, it replaces the block data structure and the mining-based data validation mechanism to offer scalability and lower transaction costs. It uses a block-lattice data structure (that is, each public key has its own blockchain which tracks its account balance, rather than their transaction amounts and can only be updated by themselves) which allows updates to take place immediately and asynchronously to the rest of the block-lattice.

Sources: Popov (2016), Baird, Harmon and Madsen (2018), Brock et al. (2018) and LeMahieu (2018)

2 Benefits and challenges of blockchain technology in tracking consumer products

This chapter discusses the opportunities and challenges that blockchain technology can bring to businesses (along the supply chain), regulators, and consumers. It starts by outlining the principle challenges faced by the supply chain industry and identifies the ways in which blockchain technology can help to address these. It then explores the main challenges and risks to the wider adoption of the technology.

The chapter ends with a high-level summary of selected problems that blockchain can help solve – from the prevention of counterfeit goods and protecting intellectual property, to ethical and environmentally sustainable practices in production, to food and pharmaceutical products meeting safety and quality standards. Further details on these applications are provided in Appendix 3: Applications of blockchain technology in tracking consumer products.

2.1 Benefits of blockchain in supply chain management

2.1.1 Current challenges faced by the supply chain industry

The supply chain industry at its most complex can be an intricate network of businesses (e.g. suppliers, manufacturers, transporters, wholesalers, retailers), organisations (e.g. trade associations, public bodies), systems, contracts, processes, and technology underlying global trade. Outsourcing, offshoring, and other globalisation pressures in the last several decades have led to an increased number of parties and unprecedented complexity in global supply chains, aggravating concerns about disruptions, delays, inefficiencies, or fraud.[32]

Managing a shared process places high demands on sharing information and trust among multiple parties. In particular:

- Businesses face new challenges of maintaining visibility into the origin, authenticity, and handling of products as they cross organisational and national boundaries.
- Regulators are facing new challenges to safeguard compliance with standards and protect public health and safety in areas such as food or pharmaceuticals.
- Consumers are becoming increasingly concerned about ethical or ecological practices in production, creating end-customer demand for supply chain transparency.

Traditional processes for supply chain management such as on-site inspections, audits, and record reconciliation are expensive and error-prone.[33] Ensuring that upstream suppliers, distributors, and transporters deliver the right product, at the right time, and in the correct manner can therefore levy a 'trust tax' on all parties.[34] An industry survey in 2017, comprising

[32] Microsoft (2018a). 'How Blockchain will transform the modern supply chain'. Published on 27 March 2018.
[33] Microsoft (2018a).
[34] Microsoft (2018a).

408 organisations from 64 countries, found that 69% do not have full visibility of supply chains, and 65% experienced at least one supply chain disruption in the past year.[35]

Contracts, transactions, and logistics processes still rely to a large extent on manual operations, which can be time consuming and susceptible to human error or fraud. There is currently little automation,[36] with only 37% of respondents in a 2017 industry survey using technology to analyse, track, or monitor potential supply chain issues. Of these, the most widely used software (41%), was Microsoft Excel.[37]

A key obstacle to better use of IT systems is the fragmentation of supply chain data. Data silos and limited data interoperability create technical difficulties for process automation, or for the provision of IT solutions that facilitate data sharing and transparency along the supply chain.

Current attempts to overcome data fragmentation largely focus on data aggregation in a centralised way,[38] but this approach raises concerns about data integrity. This is because centralised management of supply chain processes and data opens the possibility for collusion between parties and data tampering.[39] In addition, while centrally integrated IT systems can alleviate some supply chain risks, they also introduce new cyber risks. For example, the NotPetya ransomware attack in 2017 cost Maersk an estimated $300 million.[40] The top two causes of supply chain disruption identified in the 2017 industry survey were “unplanned IT or telecommunications outage” and “cyber-attack and data breach”.[41]

The following section describes the potential of blockchain technology to simultaneously address problems with both the fragmentation and centralisation of supply chain data.

2.1.2 The transformative potential of blockchain

By providing a secure tamper-proof shared data layer, blockchain can help create trust, transparency, and accountability between disparate entities in a complex supply chain.

At present, each stakeholder in the supply chain industry usually manages their own assets and data.[42] By contrast, data recorded in distributed ledgers are shared between participants. Each node in the blockchain has a copy of the whole (or partial depending on the type of blockchain) ledger and any new blocks of data appear identically for all nodes. Moreover, each network participant has visibility into the current status of products and processes, as well as all past transactions. Some permissioned networks allow companies to participate in the network while protecting their commercial interest by retaining control over who can access their data.

More importantly, blockchain technology safeguards the integrity of the data without the need of a centralised authority or intermediary. If any changes to the ledger are requested, they must be approved through a consensus mechanism[43]. Transactions and other data are stacked in blocks and appended to the existing chain of previous blocks. Information stored in

---

[35] Alcantara et al (2017). ‘BCI Supply Chain Resilience Report 2017’. Report by Business Continuity Institute (BCI) and Zurich Insurance Group (Zurich).
[36] ABI Research (2018). ‘Blockchain in the Supply Chain: Reducing Friction for Faster and More Efficient Logistics’. ABI Research Report. Q3 2018.
[37] Alcantara et al (2017).
[38] Rakic et al (2017). First purpose built protocol for supply chains based on blockchain’. Origintrail White Paper.
[39] Rakic et al (2017).
[40] ABI Research (2018).
[41] Alcantara et al (2017).
[42] ABI Research (2018).
[43] See section 2.2.2 for a formal definition.

this way cannot be later forged or modified without having to change *every* copy of the block and of all subsequent blocks.[44] Moreover, any attempt to tamper with the data will leave a record in the cryptographic audit trail. Such systems can significantly reduce the trust tax associated with traditional methods for managing shared processes.

Moreover, the use of blockchain-enabled smart contracts[45] can automate transactions, reducing the need for establishing trust before entering into commercial relationships. Pre-arranged smart contracts can trigger automatic compensation or fines based on compliance with agreed contractual obligations. Smart contracts can also communicate information, record data, or make purchases in a pre-programmed, autonomous manner. Such systems can significantly reduce the occurrence of supply chain disruptions, delays, and fraud. They could also improve efficiency and decrease waste using automated on-demand manufacturing.[46]Importantly, transparency along the full length of the supply chain simplifies product recall and supports accountability.

The innovative potential of blockchain in supply chain tracking is particularly pronounced in combination with other technologies such as Internet-of-Things[47] (IoT) and radio-frequency identification (RFID)[48] tags.[49] These sensor technologies can bring increased visibility into complex supply chains, including real-time tracking of product location and environmental conditions (e.g. temperature, humidity). Figure 4 below identifies the potential applications of distributed ledger technologies, such as blockchain, in supply chain industry. Storing this information in secure distributed ledgers safeguards the integrity of the collected data and facilitates easy information sharing between multiple parties that may include regulators as well as consumers.

The stakeholders interviewed as part of this study present varying views about the key contribution of blockchain technology to improving supply chain processes. Most agree that the technology's main potential is to bring disparate entities within a supply chain to a common, trusted network that facilitates information sharing and data accuracy.

However, stakeholders disagree about which features of the technology enable that. Some point to the decentralised governance and cryptographic elements, which ensure that data is fully traceable and immutable. Others, however, note that most existing applications are highly centralised and often rely on one dominant player or network operator.

According to a blockchain expert at the Cambridge Centre for Alternative Finance (CCAF) research institute, the success of blockchain technology in most supply chain applications is unrelated to the features of the technology itself. Rather, the hype surrounding blockchains acts as a catalyst for companies to reform inefficient legacy systems and bring multiple parties to a shared infrastructure. According to the source from CCAF, the key efficiency benefits in eliminating data silos and improving data integrity are not inherently related to blockchain and can be solved using other technological solutions.

---

[44] Section 2.2.2 provides a more detailed description.
[45] Smart contracts use computational code to execute a specified action or set of actions when certain conditions have been fulfilled.
[46] ABI Research (2017a).
[47] Internet-of-Things (IoT) is a network of inter-connected devices that interact and exchange data.
[48] A radio-frequency identification (RFID) tag is a digital label that transmits data via radio waves.
[49] Microsoft (2018a).

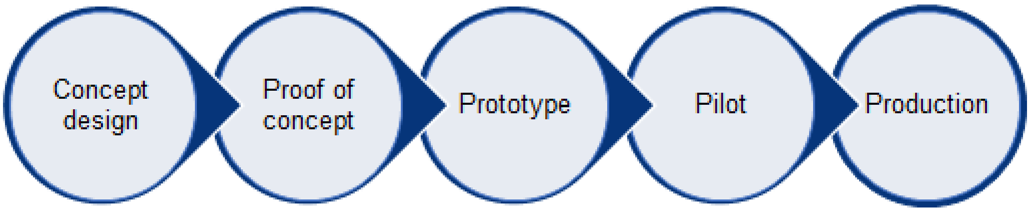
Figure 4: Blockchain applications in supply chain management

Source: ABI Research (2018). Abridged by London Economics.

2.1.3 Adoption of blockchain-based solutions

At present, blockchain-based solutions are a nascent market and most industrial applications of the technology in supply chain management are in proof-of-concept, prototype, or pilot stage of the innovative process (see Figure 5).

Figure 5: Innovation process



Source: London Economics

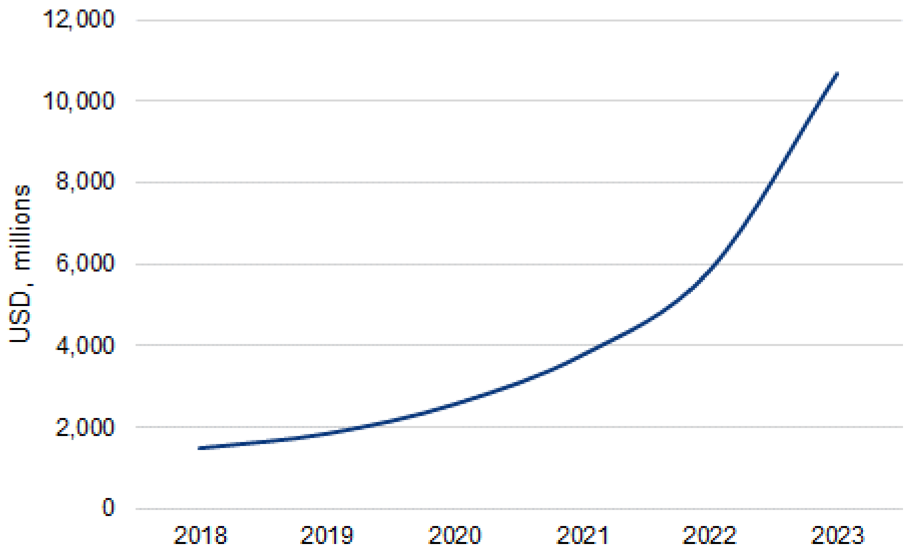
The sector is not generating significant revenues yet and some technology specialists expect a wider commercialisation and mass market reach only from 2022 onwards.[50] This is illustrated in Figure 6, which shows an estimate of the expected growth of the global revenues from activities powered by distributed ledger technologies.

A broader adoption of the technology will also depend on the results of the experiments that are being pioneered. Businesses are still in the early stages of understanding possible applications for blockchain, evaluating the potential value, and determining the commercial

50 ABI Research (2018).

viability of long-term investment.[51] Industry stakeholders that were interviewed tended to expect a mass-market reach would be achieved within approximately five years.

Figure 6: Blockchain and Distributed Ledger Revenues, World Market, Forecast 2018-2023



Note: Forecast based on venture capital funding, initial coin offerings, number of start-ups and expected sales models, number of established tech vendors offering BaaS, BaaS pricing models, average anticipated revenue for start-ups. Source: ABI Research (2018)

Interestingly, there have been mixed responses amongst various financial institutions, who have been early adopters of the blockchain technology. For example, after an initial trial using blockchain to enable real-time synchronisation of post-trade allocation and processing of trades, the Hong Kong Exchange is now launching the full service for its participants.[52] In 2018, HSBC successfully used the technology to make over 150,000 payments worth $250 million across its internal balance sheets and is now exploring how the technology can help its multinational clients.[53]

On the other hand, Ripple's chief cryptographer argued that a lack of scalability and privacy issues are preventing banks from using distributed ledger technologies.[54] Moreover, many stakeholders in the financial sector are beginning to doubt the practical use of the technology with growing concerns around its commercial viability. It has been found that proof-of-concepts demonstrate little benefit in comparison to other solutions (e.g. cloud solutions), as well as emerging views that the technology is too immature or unnecessary in specific applications.[55] According to a respondent from SAP's blockchain team, the financial industry is well ahead in understanding blockchains, but paradoxically behind on adoption. They observe less mature views in other industries, but a quicker adoption.

[51] ABI Research (2018).
[52] Finextra (2018a). 'Hong Kong Exchange preps DLT-based post-trade allocation and processing platform'. Published 31 October 2018.
[53] Finextra (2018c). 'HSBC uses DLT to settle $250bn of FX transactions'. Published 15 January 2019.
[54] Finextra (2018b). 'Ripple exec says DLT not ready for banks…yet'. Published 14 June 2018.
[55] Higginson et al (2019).

2.2 Challenges for industrial applications of blockchain

While blockchain technology has the potential to transform the supply chain industry, there are a number of risks and challenges along its path to full-scale adoption.

2.2.1 Low awareness and understanding

In the first instance, blockchain technology is generally not well understood by businesses and suffers from reputational problems. In a broad industry survey in 2017 by ABI Research, 93% of decision makers across nine industry sectors reported no familiarity with blockchain within their organisation, while 7% said early investigation of the technology was taking place. This positions blockchain as the innovative technology that is least familiar amongst industry decision makers, ranking below 5G, autonomous vehicles, augmented reality, virtual reality, artificial intelligence and others.[56]

The industry stakeholders interviewed for this study typically agree that there are considerable awareness problems, but they think the situation is quickly improving and do not consider low understanding to be a serious obstacle to widespread adoption. They note a broad interest from businesses in experimenting with the technology and a receptiveness to education. According to a source from the blockchain start-up, TE-FOOD, awareness paradoxically tends to be better in developing countries than in developed countries.

Parallels are drawn with other technologies, such as credit card payment systems, which users typically do not understand in detail but routinely rely on. The stakeholders frequently mention that trust in technology is built through proven usefulness, customer experience and broad adoption by trusted entities, notably large companies. A source from the blockchain industry association, Hyperledger, suggests that education of technologists, who have misconceived or narrow views about the technology, is more important than better understanding by ordinary users.

Misconceptions about the technology were seen as particularly concerning amongst some stakeholders, who suggested that overinflated expectations and the hype around blockchain technology can lead businesses to adopt blockchain solutions even when there is no business case for it. A source at IBM Food Trust, for example, raised these concerns, stressing that “blockchain is a technology, it’s not a solution”. In many applications, they argue, business challenges may be substantially more significant than technological challenges.

Of the approximately 86,000 blockchain projects developed since 2009, only 8% are actively maintained.[57] However, according to the respondent from Hyperledger, the main hype has already passed, and businesses are increasingly able to critically assess where blockchains add value and whether the technology is an appropriate tool to achieve their objectives.

2.2.2 Damaged reputation of cryptocurrencies

Given its inception with Bitcoin, blockchain technology is still dominantly perceived through its association with cryptocurrencies, often seen as a mere tool for illegal trade or financial speculation.[58] The damaged reputation of cryptocurrencies may have created some resistance

[56] ABI Research (2017b). ‘Industry Survey: Transformative Technology Adoption and Attitudes’. ABI Research Report. Q2 2017.
[57] Deloitte (2017a). ‘Evolution of blockchain technology’. Insights from the GitHub platform’. Article published on 6 November 2017.
[58] UK Government Office for Science (2016).

to distributed ledger technology more broadly. At the same time, however, the respondent from the Ethereum Enterprise Alliance stresses that cryptocurrencies critically helped in creating awareness about blockchains. Other stakeholders note that the negative perception is changing as businesses are relatively forgiving of new technologies and increasingly able to differentiate cryptocurrencies from other use cases.

Nevertheless, blockchain service providers often maintain an uneasy relationship with cryptocurrencies. Those who have relied on crypto-assets in their fundraising or technological solutions are wary of the reputational concerns and in some cases downplay the role of tokenised infrastructure in their marketing.[59] Meanwhile, providers that have never used crypto-tokens ensure that they highlight this fact to their customers. Some maintain that the trend of separation between blockchain and crypto-assets will continue, with the latter requiring longer time to achieve wider acceptance and adoption. Other stakeholders point to the emergence of so-called ‘stable coins’, i.e. crypto-assets whose value is pegged to fiat currencies, such as the US dollar. One stakeholder suggested that such stable coins may still be able to realise key benefits of digital tokens (such as automated micro-payments), while alleviating users’ concerns about uncertain value of the currency.

2.2.3 Implementation costs

The costs of implementing the technology could be high or largely unknown and can for some businesses conceivably outweigh the benefits.[60] In particular, the use of blockchain technology can disrupt or interfere with existing processes and business practices, creating frictions.[61] Well-established industries (such as food or pharmaceutical industries) with meticulously optimised processes may be particularly reluctant to reform.[62] On the other hand, the respondent from Everledger suggests that well-optimised companies are likely to have an already high-degree of technological competence, which can make it easier rather than harder to convert to a blockchain-based infrastructure built around the existing processes.

2.2.4 Regulatory uncertainty

Businesses may also face risks associated with early adoption arising, for example, from legal uncertainty. Regulatory regimes and legislation often lag behind technological progress, exposing businesses relying on distributed ledgers to legal vacuum or ambiguity. For example, it is unclear whether smart contracts – formulated in computer code rather than legal language – will also be legally enforceable. The transparency and immutability of data stored on blockchains can also give rise to concerns about data privacy and protection of personal data.[63]

However, regulatory risks were generally not perceived as a severe obstacle by the industry representatives that were interviewed. The respondent from Hyperledger explains that, as a technology, blockchains do not raise regulatory issues, but some of the applications of the technology are regulated – or are likely to be in the future. In particular, many stakeholders said that cryptocurrencies and fundraising through Initial Coin Offerings (ICOs) are perceived

[59] A token refers to a digital asset that serves a particular function on the blockchain. For example, cryptocurrencies have financial value and can be used for peer-to-peer transactions.
[60] Brennan et al (2018). ‘Blockchain 2.0’. Credit Suisse Equity Research. Published 11 January 2018.
[61] Deshpande et al (2017).
[62] TE-FOOD (2017c). ‘Challenges of a food traceability system implementation’. Blog post on Medium. 10 November 2017.
[63] Deshpande et al (2017).

to carry legal and regulatory risks. In the view of TE-FOOD's respondent, "Cryptocurrencies are so revolutionary that they do not fit in the traditional legal structures of countries."

By contrast, according to the respondent from SAP, in supply chain applications the regulator and the company share an interest in transparency. This enables provenance information to help the regulator safeguard compliance, while the business is better able to prevent fraud and optimise processes. A source from Blockchain Labs for Open Collaboration (BLOC), notes that regulatory requirements can be a driver of demand for blockchain-based traceability systems. For example, Modum, a Swiss blockchain start-up, helps distributors in pharmaceutical supply chains comply with new traceability regulations (see section 6.4).

It is a common view among the interviewed stakeholders that in enterprise applications of blockchains, business-related rather than technological or regulatory challenges are currently the most important obstacle to a broad adoption. Respondents from PegaSys – a blockchain development group – point to difficulties of getting competitors to work together on a shared platform. In their view, it can take time to agree on common principles and figure out a governance system, in which no one company dominates the network. Similarly, the respondent from SAP observes that a key challenge in permissioned networks is the companies' ability to find value in multi-party cooperation networks, and then to agree on the common goal, rules, and standards.

2.2.5 Lack of interoperability and security vulnerabilities

From a technological perspective, the current lack of interoperability between different distributed ledger technology implementations can lead to a fragmented ecosystem, complicating transactions and data sharing.[64] In addition, potential security vulnerabilities in the underlying code or cryptography – exposed by scandals such as the DAO hacking on the Ethereum blockchain in 2016 and the reorganisation of a series of blockchain history on Ethereum Classic in early 2019 – may lead businesses to abandon blockchain solutions and instead return to more traditional processes, the weaknesses of which are better understood.[65]

According to a source from Hyperledger, technological vulnerabilities are important but not fundamentally related to blockchain itself, but rather the specific implementation of the network. They note that all identified breaches in blockchain security arose from issues that are well known. In their view, the source of vulnerability is the implementation of the code; trust in the technology will therefore require clear accountability for failures.

In addition, there is growing concern that quantum computers will be able to hack the underlying cryptographic code, which would present a major threat to the security of blockchain technology.[66] However, new validation protocols are already being designed to be quantum-computing resistant. Cardano, a decentralised pubic blockchain and cryptocurrency project, is developing a new type of transaction which will use a quantum-resistant signature to address potential security issues. Several stakeholders highlighted the danger of quantum computing, while others dismissed it as a technological fantasy for the foreseeable future.

Businesses may also need to navigate through the trade-offs between different blockchain implementations. On the one hand, business applications relying on permissionless public blockchains may not be able to achieve mass-market reach without solving the speed and scalability problems associated with exponential growth in required computing power. On the

[64] Deshpande et al (2017).
[65] Brennan et al (2018).
[66] Higginson et al (2019).

other hand, supply chain tracking using permissioned blockchains may face doubts about trustworthiness and true data integrity given that only a small number of parties are required to validate transactions, and that the contents of the ledger can be kept private.

2.2.6 Resistance from parties that benefit from opacity

Steps to improve the transparency of supply chains may face resistance from parties who benefit from the current opacity. The global trade in counterfeit products was estimated at 5-7% of all international trade[67] with global value at around $250 billion per year.[68] However, even businesses that do not engage in outright fraud may benefit from a lack of transparency in their upstream supply chains, by being able to hide ethically or environmentally questionable sourcing practices. Many stakeholders agree that this can be a challenge in the short term, but believe that the increasing demand for transparency from downstream businesses and consumers will drive the adoption of traceability systems.

2.2.7 Data quality and integrity

Finally, the immutability property of a blockchain ensures that recorded data cannot be edited by its users in the supply chain. However, the technology on its own does not overcome the problem of inputting incorrect or fraudulent data – commonly referred to as the 'garbage in garbage out' conundrum. A source from Blockchain Labs for Open Collaboration (BLOC) considers this the key risk of blockchain applications in supply chains.

To prove the authenticity of goods, many applications are combining blockchain-based solutions with a variety of other technologies such as secure tags, seals or sensors. Electronic chips such as radio-frequency identification (RFID) tags establish a secure link between the physical product and its digital identity which reduces the risk of incorrect user input or the substitution of an authentic product with a fake. Similarly, Internet-of-Things (IoT) sensors can automatically upload in real time information about the environmental conditions of the product (e.g. temperature and humidity) on the blockchain, decreasing the danger of incorrect or fraudulent manual input. There are also some early attempts to use the shared ledger to record scientific properties that uniquely identify the product and cannot be falsified. These include, for example, face recognition of cattle or material properties of individual diamonds that are preserved even after cutting and polishing.

Several stakeholders stress the importance of other technologies alongside blockchain to protect data integrity also in the physical world. The respondent from the blockchain traceability provider Ambrosus sees the associated technologies as their key selling point that distinguishes them from competitors. Similarly, a source from the food tracking service TE-FOOD stresses that IoT technologies are essential in removing the trust issue of data entry.

However, these technologies are still underdeveloped and themselves not immune to fraud; they cannot yet completely eliminate the risk of incorrect or fraudulent data being recorded on the blockchain.

---

[67] Dennis and Kelly (2013). 'The identification of sources of information concerning food fraud in the UK and elsewhere (Q01R0025)'. Report to Defra, Food Authenticity Branch.
[68] OECD (2009). 'Magnitude of Counterfeiting and Piracy of Tangible Products: An Update'. November 2009.

Figure 7: Challenges for industrial applications of blockchain

Source: London Economics

2.3 Applications of blockchain in tracking consumer products

Table 4 provides a summary of selected problems that could potentially be solved by blockchain as well as the key identified risks and challenges faced in specific sectors which are of relevance to the Office for Product Safety and Standards (OPSS). Further details on each of these specific applications are provided in Appendix 3: Applications of blockchain technology in tracking consumer products along with real-world case studies.

Table 4: Applications of blockchain technology in tracking consumer products

Application	Solutions offered by blockchain technology	Risks and challenges
Counterfeit prevention 	● Blockchain technology can be used to track and authenticate commonly counterfeited products, such as artworks, wine, whisky, or gemstones. ● Blockchains can immutably store records of asset ownership and authenticity, reducing transaction costs and building trust. ● Ensuring product authenticity requires a secure link between the physical product and its digital	● Transparency needs must be balanced against privacy needs. ● Problems with interoperability of blockchains can undermine the permanence of authenticity certificates.

	identity. Therefore, many blockchain-based solutions combine the technology with a variety of secure tags, seals or sensors.	
Ethical & ecological sourcing 	● Increasingly, people are interested in the way products are sourced, including ethical and ecological aspects of production and distribution. ● In addition to tracking and verifying the provenance of commodities, blockchain-based solutions are also being used to address payment issues, for example in farming communities in developing countries.	● The issues underlying ethical and ecological sourcing tend to be sensitive and, in some cases, controversial. ● Commercial benefits of promoting sustainable practices may be too weak to drive broader adoption.
Intellectual property protection 	● The emergence of new digital technologies has provided consumers with many options to explore the creative arts; however, the creators must tackle the impact of the disruption on their ownership rights, opaque compensation structures and many intermediaries. ● Digital identities can be created for physical property and intangible assets, whose ownership and functioning can be controlled through smart contracts on the blockchain.	● Fragmented ecosystem that lacks interoperability between different platforms. ● Low trust in volatile cryptocurrencies. ● Inherent trade-offs between decentralisation and ease of use.
Food and pharmaceutical safety and standards 	● Two main risks to the consumer can originate from the food supply chain: (1) Safety and (2) Standards. ● Blockchain-based solutions can be used to track a product downstream from farm to store, where each participant in the network adds time-stamped transactions to a shared ledger whenever the product changes hands. The data could also include environmental and quality specifications recorded by sensors. ● Similarly, an end-to-end traceability system for pharmaceuticals can help ensure safety and quality of medicinal products.	● In some food supply chains, there may be a cost/benefit mismatch of traceability initiatives between upstream and downstream supply chain participants. ● Manually entered data can still be adulterated at input and hardware or software settings of other technologies (e.g. sensors) can be susceptible to fraud. ● Conservative and highly process-optimised industries may be averse to major disruption.

Source: London Economics

2.4 Conclusion

In their simplest form, distributed ledgers are digital databases that store information (such as records of transactions, documents, identities and assets) in such a way that they can be shared with all authorised entities in a network. The unique property of the distributed ledger architecture is that records can only be altered with the consent of other members. This gives the transparency, immutability and security of records to enable all members of a supply chain to demonstrate the provenance of goods back to their source of origin.

These distributed ledgers are based on various platforms, of which the most well-known is currently blockchain. However, care needs to be taken in the selection of distributed ledger architecture, which should be chosen according to which members have access or ability to validate records. Each option has trade-offs, especially for speed and security.

A potential weakness of many distributed ledgers is that they are still reliant on the honesty of its members to properly describe the origin of any products or processes that they add to the blockchain. In addition, there are several technical and commercial challenges to wider adoption, as shown in Table 5:

Table 5: Potential benefits and challenges to the adoption of distributed ledgers

Potential benefits	Challenges to adoption
Increased trust, transparency, and accountability between disparate entities in complex supply chains	Low awareness and understanding of the potential of the technology
Process automation through smart contracts	Implementation costs can deter firms, especially when the business value in multi-party networks is unclear
Real-time tracking and monitoring of products	Disruption of existing processes and practices, especially in highly optimised supply chains
Immutable audit trails, full transaction history	Damaged reputation of cryptocurrencies created caution about solutions relying on crypto assets
Proof of certification, identity, authenticity or compliance	Some applications may face regulatory uncertainty
Unique, shared source of truth; no data silos but also no central point of failure	Lack of interoperability between different DLT implementations
Ultimately, improved product safety and standards	Potential security vulnerabilities in the underlying code or cryptography

This report has shown the successful application of distributed ledgers in applications as diverse as counterfeit protection, ethical and ecological sourcing, intellectual property protection and the safety of food and pharmaceuticals. However, blockchain-based solutions are a nascent market, and most industrial applications of the technology in supply chain management are in proof-of-concept, prototype, or pilot stage. In many cases, it can also be argued that key efficiency gains can be achieved using other technological solutions as opposed to blockchain.

Moreover, distributed ledgers are only as good as the quality of their data. Blockchain technology alone does not solve the problem of detecting incorrect inputs. However, in combination with other technologies such as secured seals, tags and sensor technologies, it may reduce the risks arising from such challenges in the supply chain domain.

References

ABI Research (2017a). *Blockchain Applications: Beyond Fintech to the IoT.* ABI Research Report. Q2 2017. Available at https://www.abiresearch.com/market-research/product/1027514-blockchain-applications-beyond-fintech-to-/. [Accessed on 19/10/2018]

ABI Research (2017b). *Industry Survey: Transformative Technology Adoption and Attitudes.* ABI Research Report. Q2 2017. Available at https://www.abiresearch.com/market-research/product/1028244-industry-survey-transformative-technology-/. [Accessed on 05/11/2018]

ABI Research (2018). *Blockchain in the Supply Chain: Reducing Friction for Faster and More Efficient Logistics*. ABI Research Report. Q3 2018. Available at https://www.abiresearch.com/market-research/product/1031778-blockchain-in-the-supply-chain-reducing-fr/. [Accessed on 19/10/2018]

Alcantara, P., Riglietti, G., and Aguada, L. (2017). *BCI Supply Chain Resilience Report 2017*. Report by Business Continuity Institute (BCI) and Zurich Insurance Group (Zurich). Available at https://www.zurich.co.uk/_/media/dbe/united-kingdom/docs/business/corporate-and-multinational/bci_resilience_report_2017.pdf. [Accessed on 11/10/2018]

Altoros (2017). *A Close Look at Everledger - How Blockchain Secures Luxury Goods*. Published 27 April 2017. Available at https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/. [Accessed on 14/11/2018]

Ambrosus (undated). *Pharmaceutical goods quality assurance and logistics*. Available at https://ambrosus.com/assets/en/Ambrosus-Pharmacy-v2.pdf. [Accessed on 05/11/2018]

Arc-net (2017). *World First - arc-net and Adelphi's Ardnamurchan Distillery partner to put the first Scottish Spirit and Whisky on arc-net's Blockchain platform*. Press release. 27 September 2017. Available at https://arc-net.io/blog/arc-net-adelphi-partnership-blockchain/. [Accessed on 01/11/2018]

Baird, L., Harmon, M., and Madsen, P. (2018). *Hedera: A Governing Council & Public Hashgraph Network*. Hedera Hashgraph White Paper. Available at https://www.hedera.com/hh-whitepaper-v1.4-181017.pdf. [Accessed on 09/10/2018]

BBC (2013). *Q&A: Horsemeat scandal*. Published 5 February 2013. Available at https://www.bbc.co.uk/news/uk-21335872. [Accessed on 11/10/2018]

Benos, E., Garratt, R., and Gurrola-Perez, P. (2017). *The economics of distributed ledger technology for securities settlement*. Bank of England. Staff Working Paper No. 670. Available at https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.pdf. [Accessed on 02/10/2018]

Bext360 (2018). *Using Blockchain to Unlock the Supply Chain*. Article. 4 March 2018. Available at https://www.bext360.com/using-blockchain-to-unblock-the-supply-chain/. [Accessed on 15/02/2019]

BigChainDB (2016). *What is BigChainDB?.* Blog post. 14 February 2016. Available at https://blog.bigchaindb.com/what-is-bigchaindb-38aff031bf51. [Accessed on 08/11/2018]

Bocek, T., Rodrigues, B., Strasser, T., Stiller, B. (2017). *Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain*. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). Available at https://ieeexplore.ieee.org/document/7987376. [Accessed on 06/11/2018]

Bogart, S. and Rice, K. (2015). *The Blockchain Report: Welcome to the Internet of Value*. A Needham Report. Available at https://needham.bluematrix.com/sellside/EmailDocViewer?encrypt=4aaafaf1-d76e-4ee3-9406-7d0ad3c0d019&mime=pdf&co=needham&id=sbogart@needhamco.com&source=mail&utm_content=buffer0b432&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer. [Accessed on 15/10/2018]

Brennan, C., and Lunn, W. (2016). *Blockchain*. Credit Suisse Equity Research. Available at http://www.vivanest.com/wp-content/uploads/2016/09/Blockchain-The%20Trust%20Disrupter-Report%20of%20Credit%20Suisse.pdf. [Accessed on 02/11/2018]

Brennan, C., Zelnick, B., Yates, M., and Lunn, W. (2018). *Blockchain 2.0*. Credit Suisse Equity Research. Published 11 January 2018. Available at https://plus.credit-suisse.com/rpc4/ravDocView?docid=V7b2NM2AF-e. [Accessed on 15/11/2018]

Brock, A., Atkinson, D., Friedman, E., Harris-Braun, E., McGuire, E., Russell, J., M., Perrin, N., Luck, N., Harris-Braun, W. (2018). *Holo Green Paper*. March 2018. Available at https://files.holo.host/2018/03/Holo-Green-Paper.pdf. [Accessed on 09/10/2018]

Carrefour (2018). *Press Release*. 6 March 2018. Available at http://www.carrefour.com/sites/default/files/cp_carrefour_blockchain_alimentaire_06032018_ven.pdf. [Accessed on 25/10/2018]

Castro, M. (2001). *Practical Byzantine Fault Tolerance*. Massachusetts Institute of Technology. Available at https://www.microsoft.com/en-us/research/wp-content/uploads/2017/01/thesis-mcastro.pdf. [Accessed on 11/10/2018]

Cheddar (2018). *Ujo Music Founder Says Blockchain Can Fix the Music Industry*. Published 3 May 2018. Available at https://cheddar.com/videos/ujo-music-founder-says-blockchain-can-fix-the-music-industry. [Accessed on 09/11/2018]

CIPS (2017). *Case study: How Walmart uses blockchain*. Available at https://www.cips.org/supply-management/analysis/2017/june/case-study-walmart/. [Accessed on 12/11/2018]

Circulor Press Release (2018). *Circulor blockchain brings real traceability to Tantalum mined in Rwanda.* Published 16 October 2018. Available at https://www.circulor.com/rwandan-government-initiative. [Accessed on 14/11/2018]

Coinanalysis (2018). *How many transactions per second can Bitcoin Cash handle?*. Available at https://coinanalysis.io/how-many-transactions-per-second-bitcoin-cash/ [Accessed on 11/10/2018]

Coinsquare (2018). *BMW Partners with Circulor to Bring Blockchain to Ethical Sourcing.* News article. 6 March 2018. Available at https://news.coinsquare.com/business/bmw-works-circulor-source-ethical-cobalt-using-blockchain-technology/. [Accessed on 02/11/2018]

Controlant (2018). *When blockchain meets IoT and the food and pharmaceutical cold chains*. Blog post. 23 March 2018. Available at https://controlant.com/blog/2018/when-blockchain-meets-iot-and-the-food-and-pharmaceutical-cold-chains/. [Accessed on 02/11/2018]

Deloitte (2016). *Blockchain: Enigma. Paradox. Opportunity*. Deloitte LLP. Available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-fullreport.pdf [Accessed on 10/10/2018]

Deloitte (2017a). *Evolution of blockchain technology. Insights from the GitHub platform.* Article published on 6 November 2017. Available at https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html [Accessed on 15/01/2019]

Deloitte (2017b). *Using blockchain to drive supply chain innovation*. A series exploring Industry 4.0 technologies and their potential impact for enabling digital supply networks in manufacturing. Available at https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html. [Accessed on 02/10/2018]

Dennis, J. and Kelly, S. (2013). *The identification of sources of information concerning food fraud in the UK and elsewhere (Q01R0025).* Report to Defra, Food Authenticity Branch. Available at http://randd.defra.gov.uk/Document.aspx?Document=11247_FA0104-FoodFraudDeskStudy-FinalReport-1may12.pdf. [Accessed on 16/10/2018]

Deshpande, A., Stewart, K., Lepetit, L., and Gunashekar, S. (2017). *Understanding the landscape of Distributed Ledger Technologies/Blockchain*. RAND Europe. Research study funded by the British Standards Institution. Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2223/RAND_RR2223.pdf. [Accessed on: 02/10/2018]

Digiconomist (2018). *Bitcoin Energy Consumption Index*. Available at https://digiconomist.net/bitcoin-energy-consumption. [Accessed on 10/10/2018]

ETH News (2018). *Diamond Producer ALROSA Joins De Beers Blockchain Pilot*. 30 October 2018. Available at https://www.ethnews.com/diamond-producer-alrosa-joins-de-beers-blockchain-pilot. [Accessed on 09/11/2018]

Fairtrade Foundation (undated). Available at: http://www.fairtrade.org.uk/Farmers-and-Workers/Coffee

FDA (2016). *FDA Investigates Multistate Outbreak of E. coli O26 Infections Linked to Chipotle Mexican Grill Restaurants.* Available at https://www.fda.gov/food/recallsoutbreaksemergencies/outbreaks/ucm470410.htm. [Accessed on 12/10/2018]

Figure based on testing conducted with IBM in 2010. Visa (undated). *Visa acceptance for retailers*. Available at https://usa.visa.com/run-your-business/small-business-tools/retail.html [Accessed on 11/10/2018]

Financial Times (2018). *Blockchain in the art world: the pros and cons*. Published 27 July 2018. Available at https://www.ft.com/content/1c5062d8-900b-11e8-bb8f-a6a2f7bca546. [Accessed on 14/11/2018]

Finextra (2018a). *Hong Kong Exchange preps DLT-based post-trade allocation and processing platform*. Published 31 October 2018. Available at https://www.finextra.com/newsarticle/32871/hong-kong-exchange-preps-dlt-based-post-trade-allocation-and-processing-platform?utm_medium=dailynewsletter&utm_source=2018-11-1&member=20329. [Accessed on 15/10/2018]

Finextra (2018b). *Ripple exec says DLT not ready for banks…yet*. Published 14 June 2018. Available at https://www.finextra.com/newsarticle/32253/ripple-exec-says-dlt-not-ready-for-banksyet?utm_medium=dailynewsletter&utm_source=2018-6-15&member=20329. [Accessed on 15/10/2018]

Finextra (2018c). *HSBC uses DLT to settle $250bn of FX transactions*. Published 15 January 2019. Available at https://www.finextra.com/newsarticle/33207/hsbc-uses-dlt-to-settle-250bn-of-fx-transactions?utm_medium=dailynewsletter&utm_source=2019-1-16&member=20329. [Accessed on 18/01/2019]

Food Standards Agency (2011), cited in National Audit Office (2014). *Food safety and authenticity in the processed meat supply chain.* Report by the Comptroller and Auditor General. Available at https://www.nao.org.uk/wp-content/uploads/2014/10/10255-001-Food-safety-and-authenticity.pdf. [Accessed on 16/10/2018]

Food Standards Agency (2018). *FSA trials first use of blockchain*. Press Release. 2 July 2018. Available at https://www.food.gov.uk/news-alerts/news/fsa-trials-first-use-of-blockchain. Accessed on 15/02/2019.

Food, Drink & Franchise (2018*). Could blockchain and IoT enhance food safety? Q&A with Ambrosus Co-founder & CEO Angel Versetti*. Published 31 October 2018. Available at https://www.fdfworld.com/food/could-blockchain-and-iot-enhance-food-safety-qa-ambrosus-co-founder-ceo-angel-versetti. [Accessed on 05/11/2018]

Fortune (2018). *Are You Eating Sustainable Fish? Blockchain May Provide the Answer*. Published 3 January 2018. Available at http://fortune.com/2018/01/03/blockchain-cryptocurrency-sustainable-fish/. [Accessed on 15/11/2018]

Higginson, M., Nadeau, M-C., and Rajgopal, K. (2019). *Blockchain's Occam problem*. McKinsey & Company Article. Published January 2019. Available at https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem. [Accessed on 15/01/2019]

He3 Labs (2018). *Hybrid Blockchain Solutions: Real-World Combinations of Public and Private Distributed Ledger Technology (DLT)*. Blog post. 23 July 2018. Available at https://www.he3labs.com/blog/2018/7/21/hybrid-blockchain-solutions-real-world-combinations-of-public-and-private-distributed-ledger-technology-dlt. [Accessed on 02/11/2018]

IBM Food Trust Solution Brief 2.0 (2018). September 2018. Available at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=89017389USEN. [Accessed on 24/10/2018]

IFPI (2018). *Global Music Report 2018: State of the Industry*. Available at https://www.ifpi.org/downloads/GMR2018.pdf. [Accessed on 07/11/2018]

IG (2018). *The tangle vs blockchain: A comparison between IOTA and bitcoin*. Published on 9 July 2018. Available at https://www.ig.com/uk/trading-opportunities/the-tangle-vs-blockchain--a-comparison-between-iota-and-bitcoin-180709. [Accessed on 09/10/2018]

ILT (2017). *Use case Blockchain: Rij- en rusttijden*. ILT Report. Available at http://cdn.instantmagazine.com/upload/6826/blockchain-ilt-02.4ea1481b14d2.pdf. [Accessed on 12/11/2018]

JCK Blogs (2018). *Inside Tracr, the De Beers-Developed Blockchain Platform*. 29 June 2018. Available at https://www.jckonline.com/editorial-article/tracr-de-beers-blockchain-platform/. [Accessed on 09/11/2018]

LeMahieu, C. (2018). *Nano: A Feeless Distributed Cryptocurrency Network*. Nano White Paper. Available at https://nano.org/en/whitepaper. [Accessed on 09/10/2018]

Microsoft (2018a). *How Blockchain will transform the modern supply chain*. Published on 27 March 2018. Available at https://azure.microsoft.com/en-gb/resources/how-blockchain-will-transform-modern-supply-chain/en-us/. [Accessed on 11/10/2018]

Microsoft (2018b). Bühler will track crops from farm to fork using blockchain technology. Microsoft Industry Blogs. Published 25 September 2018. Available at https://cloudblogs.microsoft.com/industry-blog/manufacturing/2018/09/25/buhler-will-track-crops-from-farm-to-fork-using-blockchain-technology/. [Accessed on 11/10/2018]

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at https://bitcoin.org/bitcoin.pdf. [Accessed on 02/10/2018]

O'Dair, M., Beaven, Z., Neilson, D., Osborne, R., and Pacifico, P. (2016). *Music on the Blockchain.* Blockchain For Creative Industries Research Cluster, Middlesex University, Report Nº 1. Available at https://www.mdx.ac.uk/__data/assets/pdf_file/0026/230696/Music-On-The-Blockchain.pdf. [Accessed on 08/11/2018]

OECD (2007). *The Economic Impact of Counterfeiting and Piracy*. OECD Report. Available at https://www.oecd.org/sti/38707619.pdf. [Accessed on 02/11/2018]

OECD (2009). *Magnitude of Counterfeiting and Piracy of Tangible Products: An Update.* November 2009. Available at https://www.oecd.org/sti/ind/44088872.pdf. [Accessed on 02/11/2018]

Pharmaceutical Commerce (2018). *The 2018 market for pharma cold chain logistics is $15 billion*. Article. Published 8 May 2018. Available at http://pharmaceuticalcommerce.com/clinical-operations/the-2018-market-for-pharma-cold-chain-logistics-is-15-billion/. [Accessed on 16/10/2018]

Popov, S. (2016). *The tangle*. IOTA White Paper. Available at: http://www.tangleblog.com/wp-content/uploads/2016/11/IOTA_Whitepaper.pdf. [Accessed on 09/10/2018]

Provenance (2015). *White Paper*. Available at https://www.provenance.org/whitepaper. [Accessed on 31/10/2018]

Provenance (2016). *From shore to plate: Tracking tuna on the blockchain.* Available at https://www.provenance.org/tracking-tuna-on-the-blockchain#overview. [Accessed on 31/10/2018]

PwC (2015). *Food Fraud Vulnerability Assessment and Mitigation*. Report 2015. Available at https://www.pwc.com/gx/en/services/food-supply-integrity-services/assets/pwc-food-fraud-vulnerability-assessment-and-mitigation-november.pdf. [Accessed on 05/10/2018]

PwC (2016). *Digitization in pharma: Gaining an edge in operations.* PwC Report. Published 19 October 2016. Available at https://www.strategyand.pwc.com/media/file/Digitization-in-pharma.pdf. [Accessed on 05/11/2018]

Rakic, B., Levak, T., Drev, Z., Savic, S., and Veljkovic, A. (2017). *First purpose built protocol for supply chains based on blockchain*. Origintrail White Paper. Available at https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf. [Accessed on 01/11/2018]

Rethink Music (2015). *Fair Music: Transparency and Payment Flows in The Music Industry*. Rethink Music Initiative. A project of Berklee Institute of Creative Entrepreneurship. Available at https://www.berklee.edu/sites/default/files/Fair%20Music%20-%20Transparency%20and%20Payment%20Flows%20in%20the%20Music%20Industry.pdf. [Accessed on 07/11/2018]

Roberson, C. (2015). *Innovation in global cold chain transport is helping to reduce food and medical waste*. TradeReady Blog. Published 17 September 2015. Available at http://www.tradeready.ca/2015/trade-takeaways/innovation-global-cold-chain-transport-helping-reduce-food-medical-waste/. [Accessed on 11/10/2018]

Rosengart, K. (2017). *De Beers Turns Down Participation GIA Diamonds Provenance Program.* Blog post. 29 August 2017. Available at https://blog.krosengart.com/de-beers-turns-down-participation-gia-provenance-program. [Accessed on 09/11/2018]

Sawtooth (undated). *Bringing traceability and accountability to the supply chain through the power of Hyperledger Sawtooth's distributed ledger technology*. Available at: https://sawtooth.hyperledger.org/examples/seafood.html. [Accessed on 09/10/2018]

Spink, J. (2014), cited in PwC (2015). *Food Fraud Vulnerability Assessment and Mitigation*. Available at https://www.pwc.com/gx/en/services/food-supply-integrity-services/assets/pwc-food-fraud-vulnerability-assessment-and-mitigation-november.pdf. [Accessed on 02/11/2018]

Supermarket News, (2018), *More retailers join IBM Food Trust network*. Available at https://www.supermarketnews.com/food-safety/more-retailers-join-ibm-food-trust-network. [Accessed on 02/02/2019]

Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. [Accessed on 04/10/2018]

TE-FOOD (2017a). *White paper*. Available at https://ico.tefoodint.com/te-food-white-paper.pdf. [Accessed on 05/11/2018]

TE-FOOD (2017b). *TE-FOOD – Modum comparison*. Blog post on Medium. 18 December 2017. Available at https://medium.com/te-food/te-food-modum-comparison-3a98c1745718. Accessed on 05/11/2018]

TE-FOOD (2017c). *Challenges of a food traceability system implementation*. Blog post on Medium. 10 November 2017. Available at https://medium.com/te-food/challenges-of-a-food-traceability-system-implementation-b0bf91453571. [Accessed on 01/11/2018]

The Guardian (2017). *UK's top supplier of supermarket chicken fiddles food safety dates*. Article. Published 28 September 2017. Available at https://www.theguardian.com/business/2017/sep/28/uks-top-supplier-of-supermarket-chicken-fiddles-food-safety-dates. [Accessed on 11/10/2018]

Ujo Music (2018a). *Introducing Ujo Portal: Making Musicians More Money*, Blog published 13 December 2018. Available at https://blog.ujomusic.com/introducing-ujo-portal-making-musicians-more-money-9224d808a57a. [Accessed on 20/02/2018]

Ujo Music (2018b). *The Ujo Platform: A Decentralized Music Ecosystem*. Blog post. Published 3 July 2018. Available at https://blog.ujomusic.com/the-ujo-platform-a-decentralized-music-ecosystem-e530c31b62bc. [Accessed on 09/11/2018]

UK Government Office for Science (2016). *Distributed ledger technology: beyond block chain*. A report by the UK Government Chief Scientific Adviser. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. [Accessed on: 02/10/2018]

UNOPS and Blockchainpilots.nl (2018). *The legal aspects of blockchain*. Published on 26 September 2018. Available at https://www.blockchainpilots.nl/books. [Accessed on 16/01/2019].

US Food & Drug Administration (2016). *FDA Investigates Multistate Outbreak of E. coli O26 Infections Linked to Chipotle Mexican Grill Restaurants*. Report. 1 February 2016. Available at https://www.fda.gov/food/recallsoutbreaksemergencies/outbreaks/ucm470410.htm#what. [Accessed on 15/10/2018]

Voshmgir, S. and Kalinov, V. (2017). *Blockchain Handbook: A Beginners Guide*. Available at https://s3.eu-west-2.amazonaws.com/blockchainhub.media/Blockchain+Technology+Handbook.pdf. Accessed on 08/11/2018]

Walmart (2018), Letter to Leafy Greens Suppliers. Available at https://corporate.walmart.com/media-library/document/blockchain-supplier-letter-september-2018/_proxyDocument?id=00000166-088d-dc77-a7ff-4dff689f0001. [Accessed 01/03/2019]

WHO (2006). *Counterfeit Medicines: an update on estimates 15 November 2006*. Updated 14 February 2018. Available at http://www.who.int/medicines/services/counterfeit/impact/TheNewEstimatesCounterfeit.pdf. [Accessed on 02/11/2018]

WHO (2017). *Food safety*. Available at http://www.who.int/en/news-room/fact-sheets/detail/food-safety. [Accessed on 12/10/2018]

World Bank Group (2017). *Distributed Ledger Technology (DLT) and Blockchain*. FinTech Note Number 1. Available at http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf. [Accessed on 02/10/2018]

World Economic Forum (2015). *Deep Shift: Technology, Tipping Points and Societal Impact.* Survey Report. Available at http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. [Accessed on 08/11/2018]

XRP Ledger Documentation. Available here: https://developers.ripple.com/docs.html. [Accessed on 11/10/2018]

3 Appendix 1: Other consensus mechanisms

Alternative algorithms to reach consensus have been developed to overcome weaknesses (such as scalability and resource wastefulness) in the Proof-of-Work algorithm that was initially developed for Bitcoin. Some examples are briefly summarised in Table 6.

Table 6: Other consensus mechanisms

Consensus mechanism	Description
Proof-of-Stake (PoS)	Validators are chosen in a deterministic way based on their stake. In early PoS implementations, the stake was simply a user's amount of the underlying cryptocurrency. The rationale was that users who have acquired more of the cryptocurrency have a greater interest in ensuring its success and are thus less likely to act maliciously. In order to avoid the richest user being selected every time, a random element is also added to the selection process. Successful validators are rewarded in the form of transaction fees these systems as opposed to payment in cryptocurrency. This mechanism has been criticised for being less secure, particularly as users in early implementations did not actually lose any part of their stake if they acted in a malicious way.
Practical Byzantine Fault Tolerance (PBFT)	A consensus algorithm that tolerates malicious nodes (so called Byzantine faults), originally developed by Miguel Castro and Barbara Liskov at the MIT. Consensus is reached via communication by all nodes. One node takes the role of primary node, with all other nodes being referred to as the backup nodes. The algorithm broadly works in four steps: When a client wants to invoke an operation (e.g. a transaction), they send a request to the primary node. The primary node then sends this request to all backup nodes. The backup nodes process the request and send an authenticated reply directly to the client. The client waits until it has received f+1 replies (where f represents the maximum number of nodes that are tolerated to be faulty or malicious) with correct authentication from different backup nodes with the same result. Once the client has received f+1 replies with the same result, this is the final result of the operation. In this way the honest nodes can reach an agreement on the result of the operation, even in the presence of up to f faulty nodes. PBFT overcomes the scalability and energy efficiency problems present in Proof of Work implementations; in this case by reaching consensus via communication by all nodes. PBFT works very well in smaller networks, however, due to the vast amounts of communication required between nodes, the algorithm performs less well in larger systems. PBFT implementations are also susceptible to attackers who manage to gain control over f+1 nodes, allowing attackers to trick the system into accepting results of their choice.
Proof-of-Authority (PoA)	A relatively new permission-based consensus algorithm that requires nodes to be authorised in order to be able to validate blocks. This gives the owner of the blockchain the ability to only approve those nodes that they are confident will not act in a malicious way. Authorisation can be granted based on a number of factors, for example by verifying the identity of users wishing to be approved.
Ripple	Ripple is based on blockchain but has developed its own consensus algorithm which significantly improves on the transaction speed of Bitcoin, currently

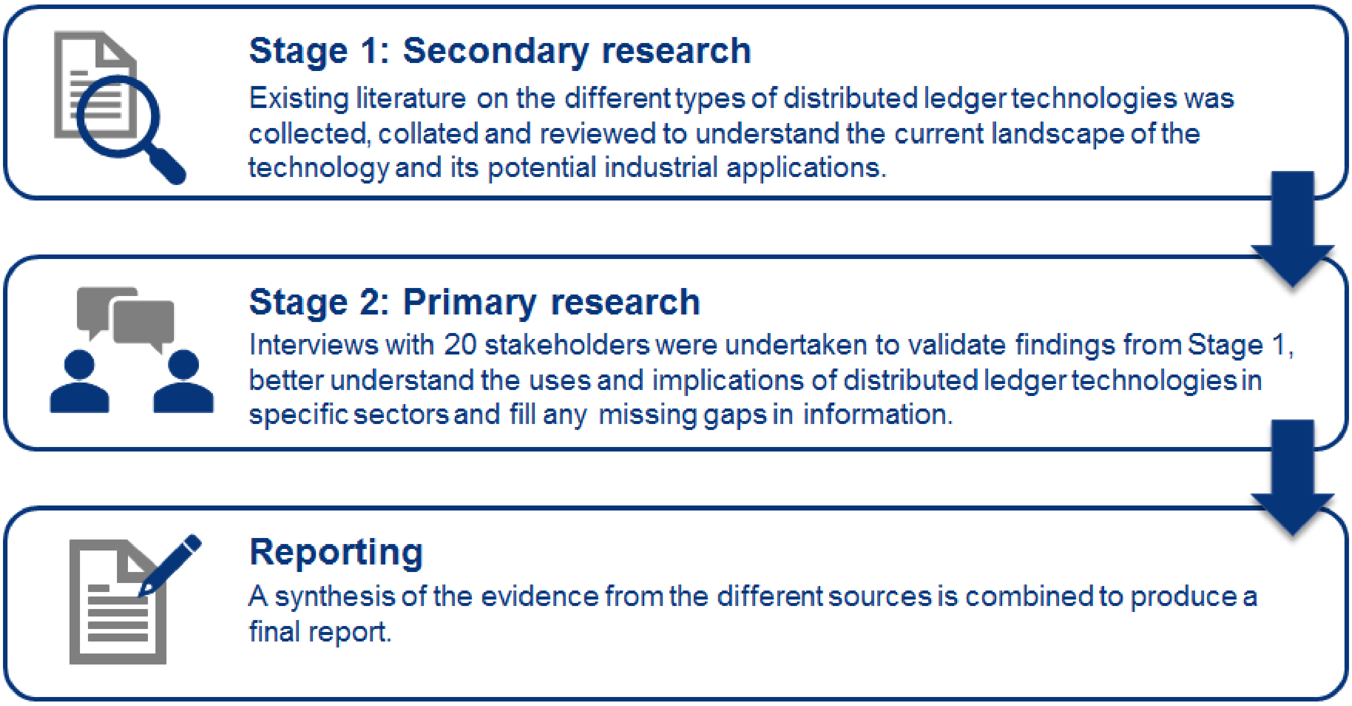
Consensus mechanism	Description
	processing 1,500 transactions per second. Ripple has two types of nodes; client nodes, which only allow a user to send and receive transactions, and server nodes which are responsible for validating transactions using the Ripple Protocol Consensus Algorithm (RPCA). The RPCA works in rounds: At the beginning of each round, all servers take all valid but not yet validated transactions and puts these into a candidate set. The server itself also has a list of servers it trusts, called unique node list. Once each server has compiled their candidate set, it contacts the servers in its unique node list and combines its candidate set with that of these servers. The servers then vote on all transactions. Transactions that receive more than a pre-defined threshold of votes are moved onto the next round. In the final round, Ripple requires at least 80% of the servers within a server's unique node list to approve the transaction. Once approved, transactions are placed on the ledge, which is then closed.

Sources: Benos, Garratt, and Gurrola-Perez (2017), Castro (2001), Microsoft (2018a). XRP (Ripple) Ledger Documentation.

4 Appendix 2: Study methodology

The objectives of this research study were addressed using a two-stage approach, as illustrated in Figure 8. This approach developed the existing knowledge and understanding of the current landscape of distributed ledger technologies and their applications in key areas and sectors. The findings were tested and validated by consulting key stakeholders. Each stage is described in more detail below.

Figure 8: Two-stage methodological approach



4.1 Stage 1: Secondary research

To identify the different types and uses of distributed ledger technologies, a thorough review of the existing literature was undertaken. The aim of this stage was to establish a deeper understanding of the different types of distributed ledger technologies that exist and identify practical examples of their use in specific sectors alongside the potential opportunities and challenges that have emerged from adopting the technology. The review process can be broken down into three key phases:

1. **Develop a list of key search terms and identify potential sources:** Evidence (in the form of empirical research, business surveys, interviews with key stakeholders, etc.) provided from research commissioned and published by UK and non-UK government departments, other public bodies, representative organisations/associations, consultancies and research centres, was sourced using key search terms (such as ‘UK government blockchain’, ‘blockchain in supply chain management’, etc.) in Google Search and Google Scholar. In addition, any relevant evidence made available by users or providers of blockchain technology as well as technology experts (e.g. blog posts, white papers and news posts) were also considered. Moreover, to ensure that all relevant literature was considered, in a second step, relevant citations referred to in each of the articles were assessed to identify any additional relevant sources.

2. **Develop and apply exclusion criteria:** After phase 1 was completed, the project team screened each document to assess its appropriateness in addressing the study objectives. Each source was also examined for any potential bias and excluded to ensure the information presented reflected the current state of play in relation to distributed ledger technologies and their applications.
3. **Perform a detailed review:** The final phase of the literature review consisted of a full-scale review of the collected information in relation to the research's objectives, identifying the different types of distributed ledger technologies, their relative advantages and disadvantages, key users and providers in specific industrial applications, areas of uncertainty in relation to the technology, as well as any gaps in the collated evidence.

In conjunction with the literature review, the collated evidence was also used to produce six short case studies covering a range of use cases of the technology.

4.2 Stage 2: Primary research

One of the main objectives of the research study was to identify specific success factors, opportunities and challenges presented in particular industries using blockchain to track and verify the provenance of consumer products. In order to achieve a deeper understanding and to validate and enrich the emerging findings from Stage 1, 20 interviews were conducted with a wide range of stakeholders in the blockchain ecosystem, including 15 service providers, two users, three industry associations and researchers.

These interviews explored key areas of interest such as:

- Perceptions of what makes blockchain technology disruptive.
- Awareness and assessment of the main opportunities and challenges for the industrial applications of blockchain.
- Insights into their specific role in the blockchain ecosystem and views on the use of the technology in the supply chain industry.

Prior to each interview, all interviewees were sent information about the aims of the project and the purpose of the interview. An interview guide was designed and used. The guide included a set of general questions asked to all interviewees as well as tailored questions depending on the stakeholder group. Interviews lasted between 30 and 45 minutes.

5 Appendix 3: Applications of blockchain technology in tracking consumer products

5.1 Counterfeit prevention

5.1.1 Current situation and problems

The OECD estimates the global value of counterfeiting at around $250 billion per year[69], which represents 5-7% of global trade.[70]

High-value and luxury goods tend to be some of the most commonly counterfeited products.[71] Examples include artworks, wine, whisky, or gemstones. In the markets for such goods, authenticity and product identity are usually inseparable from brand value. Producers are therefore particularly concerned with ways to certify authenticity of their products. Several stakeholders reported that the threat of fraud and increasing consumer demand for transparency in these high-value goods sectors are the main drivers of demand for blockchain-based traceability solutions.

Proof of authenticity is also important to support insurance claims. If, for example, a fire in the home of an art collector destroys not only the artworks but also the documents of ownership, settling an insurance claim could be complicated. If the art collector's proofs of purchase, provenance of works in their collection and all related legal and insurance documents are held on a secure, permanent, trusted database, settling insurance and similar claims becomes considerably easier.[72]

5.1.2 Solutions offered by blockchain

Several blockchain technology start-ups focus specifically on attesting provenance of frequently counterfeited consumer products. Shared ledgers can be used to track the product's digital identity through the full supply chain, while the immutability of the blockchain prevents any data alterations.

However, ensuring product authenticity also requires a secure link between the physical product and its digital identity. Many blockchain-based solutions therefore combine blockchain technology with a variety of secure tags, seals or sensors. There are also some early attempts to use the shared ledger to record scientific properties that uniquely identify the product and cannot be falsified.[73]

---

[69] OECD (2009).
[70] World Customs Organisation, (WCO) (2004), cited in Dennis and Kelly (2013).
[71] OECD (2007). 'The Economic Impact of Counterfeiting and Piracy'. OECD Report.
[72] Financial Times (2018). 'Blockchain in the art world: the pros and cons'. Published 27 July 2018.
[73] See, for example, the description of Tracr in the following section.

5.1.3 Specific application(s)

5.1.3.1 Tracking the provenance of diamonds

The fast-growing British start-up, **Everledger**, offers a blockchain-based solution for tracking the provenance of diamonds, gemstones, art or luxury goods. Powered by IBM Blockchain since 2016, the service enables businesses within a supply chain to use a shared ledger that tracks assets as they move across the value chain. According to Everledger CEO Leanne Kemp, problems related to fraud, document tampering, synthetic stones, black markets, or conflict stones are rooted in low supply chain visibility and a paper-based certification system.[74]

The shared digital ledger provided by Everledger can help address these issues, which are reportedly worth $50 billion every year, and are reflected in the increased cost of insurance.[75] The respondent from Everledger, notes that the company's product is already in production stage with a number of clients. Everledger's main customers include the full range of companies along the diamond supply chain (e.g. mining companies, manufacturers, jewellery factories, traders, and retailers). More recently, the company also started tracking coloured gemstones and luxury wines.

Tracr

Setting the standard for diamond traceability

Mission

Tracr was conceived in 2017 by De Beers, the world's largest diamond company, as a mine-to-customer traceability solution for the diamond industry. According to the company, Tracr is the first collaborative, industry-focused digital platform that securely tracks a diamond across the full value chain. The programme is intended not only to allow companies to track their supply and prove the provenance of products, but also assure consumers that the diamonds they are purchasing were mined under acceptable conditions.[76]

The precise governance structure of the initiative is still yet to be finalised. De Beers has already announced Tracr will be eventually governed by an independent foundation.[77]

Use of distributed ledger technologies

Unlike some other blockchain initiatives for tracking gemstones, Tracr will not rely on company record-keeping. Instead it uses scientific data to uniquely identify each diamond, even as it moves from its rough to polished form.[78] Each unique fingerprint is stored on the Ethereum blockchain, which is shared among the industry participants. As the diamond moves along the supply chain, all transactions are added to the ledger, creating a complete record of the diamond's full history.

The uploaded data will create a tamper-proof trail of a diamond's journey along the value chain. However, according to the Tracr website, a privacy technology will be employed that allows users to own their data and share it selectively. The technological solution should

[74] Altoros (2017). 'A Close Look at Everledger - How Blockchain Secures Luxury Goods'. Published 27 April 2017.
[75] Altoros (2017).
[76] ETH News (2018). 'Diamond Producer ALROSA Joins De Beers' Blockchain Pilot'. 30 October 2018.
[77] JCK Blogs (2018).
[78] JCK Blogs (2018)

ensure immutable traceability, while at the same time allowing individual participants to restrict access to sensitive commercial data.

Given that Tracr is based on Ethereum, the platform will also create opportunities for participants to build their own applications on top of the blockchain layer, which will include use of the information in the ledger.

Progress to date

The pilot project, involving a small group of industry participants, launched in January 2018 and has so far been able to track and identify 200 different diamonds.[79] In October 2018, the pilot was joined by Alrosa, the world's second largest diamond producer after De Beers. Tracr is currently engaging with stakeholders including diamond producers, industry trade associations, graders, governments, logistics providers, retailers and banks, to develop an inclusive and open governance structure.

Opportunities

A full traceability of individual diamonds can provide consumer assurance of origin and ethical sourcing. Tracr could also help companies fulfil their know-your-customer (KYC) obligations to banks and reduce costs in diamond insurance.[80] Under the current conditions, diamonds need to be tested at every step of the pipeline, but the use of blockchain-backed information would lessen the need for this.

Challenges

De Beers recently attracted controversy by refusing to participate in a mine-to-market provenance initiative under which the company would allow supply chain partners to trace specific goods back to De Beers.[81] The company also typically does not disclose the country of origin when selling its diamonds. This historical lack of commitment to full transparency may raise questions about De Beers' determination to provide information to consumers through Tracr. The planned blockchain structure will allow individual participants to keep information private, and a decision has not yet been reached regarding how much of the data stored on the blockchain will be available to consumers.[82]

5.1.3.2 Other notable examples

Another collaborative initiative, **TrustChain**, brings together IBM and a consortium of diamond and jewellery companies to track and authenticate diamonds, precious metals, and jewellery from mine to the retailer. The project is currently in a proof of concept stage, which should see a set of six engagement rings fully traced through the supply chain process.[83]

The risk of errors, omissions and fraud is also pronounced in the art market, partially due to the absence of a unique authority that could settle authenticity or ownership disputes. One of the companies that try to address this need is **Verisart**, a platform to certify and verify artworks and collectibles using the Bitcoin blockchain. According to a source from Verisart, they have over 40,000 artists who use the platform to generate certificates of authenticity. The artists could also choose additional datapoints to be part of the record, such as an electronic tag,

[79] JCK Blogs (2018)
[80] JCK Blogs (2018)
[81] Rosengart (2017). 'De Beers Turns Down Participation GIA Diamonds Provenance Program'. Blog post. 29 August 2017.
[82] JCK Blogs (2018).
[83] TrustChain website. Available at: https://www.trustchainjewelry.com/. [Accessed on 02/11/2018]

unique fingerprint, or multispectral image that secure the link between the physical asset and its digital identity.

The blockchain start-up, **Blockverify**, plans to combat counterfeiting by introducing transparency in the supply chains of luxury items, electronics, and diamonds.[84] **Arc-net**, discussed in greater detail below, uses distributed ledgers to authenticate whisky.

5.1.4 Risks and challenges

Blockchain technology does not fully eliminate the need for a trusted third party. For example, to prevent fraudulent ownership claims being logged to the immutable blockchain, companies such as Verisart only allow registration of artworks by artists that are first verified through conventional means. Blockchain solutions for high-value assets must also find a balance between transparency (to prove authenticity or ownership) and privacy needs. The respondent from Verisart cautions that owners of, for example, high-value art and collectibles do not necessarily want their ownership to be public.

Blockchain's current problems with interoperability of different protocols can undermine the permanence of ownership and provenance records. According to the source from Verisart, it may be difficult in the future to carry over records from one blockchain network to another. The data stored on the blockchain may therefore be tied to a specific legacy network, which can become outdated over the longer-term.

5.2 Ethical and ecological sourcing

5.2.1 Current situation and problems

The reasons why consumers care about the provenance of products go beyond safety and authenticity. Increasingly, people are also interested in the way the product was sourced, including ethical and ecological aspects of production and distribution. Among other concerns, this can include environmental damage, ecosystem disruption, exploitative extraction conflict resources[85], child labour, unsafe working conditions or resource waste. People may also be interested in the ultimate origin of goods, including intermediate stages, when taking part in consumer boycotts of products that are sourced from a country or organisation whose practices do not align with the consumer's values.

In the UK, 30% of people are concerned about issues regarding the origin of products but struggle to act on this through their buying decisions.[86] Existing sustainability standards and certifications (e.g., Fairtrade or Forest Stewardship Council) have been an important tool to enable ethical consumption but the meaning of such labels can be opaque and difficult to verify.[87]

5.2.2 Solutions offered by blockchain

In response to growing regulatory requirements, as well as social, environmental and governance challenges and opportunities, several technology solutions for product provenance are explicitly directed at proving ethical and environmentally sustainable practices. In addition

[84] Blockverify website. Available at: http://www.blockverify.io/. [Accessed on 02/11/2018]
[85] Conflict resources are natural resources extracted in a conflict zone and sold to perpetuate the fighting.
[86] Provenance (2015). "White Paper".
[87] Provenance (2015).

to using blockchain technology to track and verify provenance of commodities such as precious metals, conflict minerals, consumed foods (e.g. livestock, seafood, coffee, cocoa and vanilla) and lumber, the technology is also being used to address payment issues which are particularly prevalent in farming communities in developing countries. In many cases, upstream suppliers are forced to accept low prices and delayed payments for their products, affecting their ability to provide the basic necessities for their families.

Blockchain-based solutions make it possible for all parties involved in a transaction (e.g. farmers, companies, consumers, lenders and regulators) to access data transparently and for upstream suppliers (e.g. farmers) to be paid in real-time. Combined with other technologies such as machine vision, artificial intelligence (AI) and IoT devices, the blockchain technology also enables a more efficient evaluation of the quality of commodities received at each stage of the supply chain. This reduces the costs associated with the certification process and enables prompt upstream payment.

Blockchain-based methods for ensuring proper conduct have also been explored by some regulators.

5.2.3 Specific application(s)

Human Environment and Transport Inspectorate

Tracking of working and resting hours of lorry drivers in The Netherlands

Mission

In recent years, more than 30 Dutch government organisations concluded blockchain pilots.[88] The Human Environment and Transport Inspectorate (ILT), a government agency protecting safe and sustainable living environments, developed a blockchain-based system for the tracking of working and resting hours of lorry drivers. The scheme aimed to make regulatory supervision far more comprehensive and reliable, while at the same time reducing administrative costs.

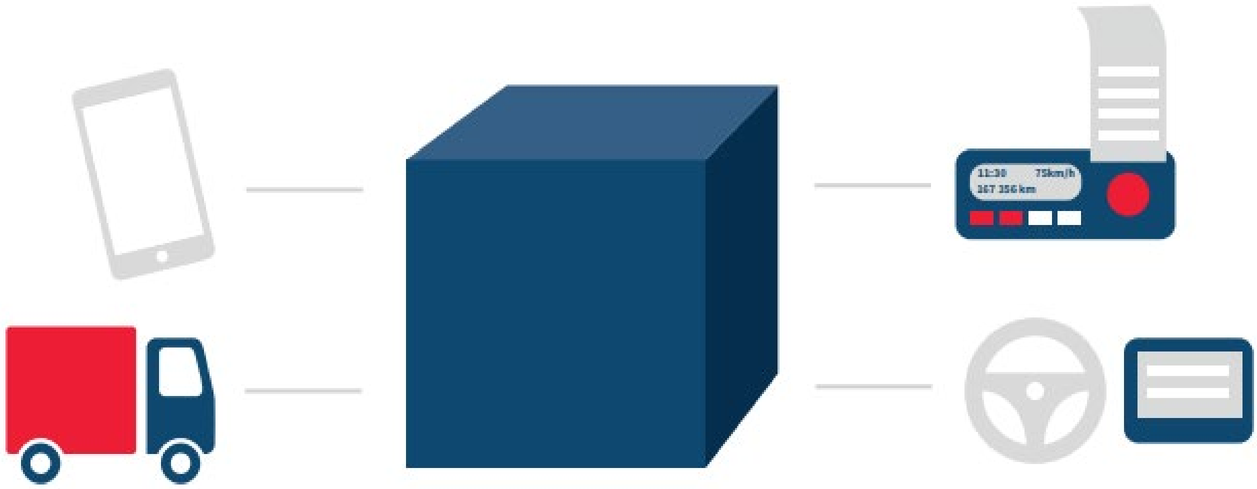
Simultaneously, the agency is also testing blockchain technology in the transport of toxic waste, seeking to promote secure data sharing and more efficient administrative procedures in multi-stakeholder process management.

Use of distributed ledger technologies

The data of driving and rest times of lorry drivers are already digitally recorded by their tachograph, but this is only provided to the ILT on request.[89] Moreover, there are several ways in which the tachograph data can be manipulated by the driver or the company. This uncertainty with the integrity of the received data means that ILT also employs physical road checks.

[88] UNOPS and Blockchainpilots.nl (2018). “The legal aspects of blockchain”. Published on 26 September 2018.
[89] According to the ILT, 650 companies are requested to provide data on driving and rest times every year. This compares with 12,000 transport companies operating in the Netherlands and a further 30,000 companies, for whom transport is only a secondary activity but who still have to monitor driving and rest times of drivers (ILT, 2017).

The piloted blockchain solution would give the ILT direct access to the digitally recorded data, in real time, making compliance checking much easier. At the beginning of the journey, the driver logs the journey via a mobile app, and then all information from this and the tachograph is transmitted and stored on a blockchain. The blockchain then provides a tamper-proof and transparent log of events.



Regulatory compliance is assessed automatically using a smart contract that compares the recorded data with administrative obligations for driving and rest times.

Progress to date

A pilot involving a small number of companies was completed in the first half of 2017. The project has since been discontinued due to technical problems and insufficient cooperation from transport companies.

The ILT is considering other processes for protecting safety and standards that can be simplified and automated using sensor data stored on blockchain. This might include the weighing of cargo via road surface sensors or checking the transport of dangerous goods by tracking lorries carrying dangerous goods signs in adverse weather conditions.[90]

Opportunities

Direct access to the digitally recorded driving and resting times would allow the ILT to monitor compliance on a much larger scale. The automation of inspections would also reduce administrative expenses. Moreover, if the tachographs are equipped with anti-tampering features and the governance of the shared ledger is set up in a way that guarantees its immutability, the resulting data would be reliable. This would allow the ILT to reduce physical road inspections.

In addition, the ILT planned to rank transport companies according to compliance and make the list publicly available. The potential bad publicity could be a further incentive for companies to ensure their drivers observe prescribed rest times.

[90] ILT (2017). 'Use case Blockchain: Rij- en rusttijden'. ILT Report.

Control of driving and rest times is an expense for the regulator and for the transport companies. The use of a shared secure ledger to prove compliance can therefore offer benefits to the firms as well.

Challenges

The envisaged participation of transport companies in the shared ledger is voluntary. The companies lack of willingness to cooperate is one of the key reasons why the project was abandoned after the first pilot. According to the ILT, the initiative could help the agency cut costs and ensure compliance even if some companies do not participate.

5.2.3.1 Authenticity and ethical sourcing of consumed goods

Founded in 2015, **bext360** uses blockchain technology to improve social sustainability aspects in critical supply chains including coffee, cotton, essential oils, minerals, cocoa and honey producers. Approximately 80% of coffee globally is produced by 25 million small-scale farmers in South America, Africa and Asia;[91] however, the chain of information regarding authenticity of the proclaimed quality of coffee beans and the treatment of farmers is opaque (in some cases, un-digitalised) and subject to falsification.

Bext360's first product integrated blockchain technology with machine learning and AI to evaluate and sort coffee cherries and beans based on their quality. Farmers were then able to use a mobile application, powered by blockchain, to view payment offers based on coffee quality. They then have the option to accept or reject the proposed payment, which is made immediately upon acceptance. Information for each evaluation and transaction is stored on the blockchain, which also records the farmer's identity, product quality, downstream purchasers and payments made. This allows end-to-end visibility in the supply chain.[92]

Moreover, farmers also have the ability to connect their other accounts to the mobile application for transactions such as loan repayments, local taxes and other financial commitments, allowing them to better manage their finances. After completing pilots in California and Uganda, bext360 now has active projects with multi-national companies in the coffee industry and has also successfully implemented its solution in the cotton and cocoa industry.

Interestingly, bext360 also uses blockchain technology to create tokenised assets (crypto-assets) reflecting the value of the underlying commodity. This allows all stakeholders across the supply chain to own tokens, which can be used as a method of payment (using smart contracts) and hold real value for financial institutions. In cases where the producer cannot receive a digital payment, blockchain is also able to create a digital receipt recording key information.

5.2.3.2 Authenticity and ethical sourcing of conflict minerals

A London-based start-up, **Circulor**, provides blockchain solutions for supply chain tracking of consumer electronics.

In one of its pilots, the firm partnered with BMW to prove that batteries for its electric vehicles contain ethically sourced cobalt. Around two thirds of the world's supplies of cobalt are from

[91] Fairtrade Foundation website (undated).
[92] Bext360 (2018). "Using Blockchain to Unlock the Supply Chain". Article. 4 March 2018.

Democratic Republic of Congo, sourced from unregulated artisanal mines where child labour is suspected to be used.[93]

More recently, Circulor started a project with the Rwandan government to record the provenance of tantalum mined in Rwanda, the world's largest producer of the metal. The objective is to bring greater transparency to the tantalum supply chain, and to help companies comply with the internationally mandated efforts to eradicate sources of funding for conflict minerals.[94]

Similarly, the diamond mine-to-customer traceability solutions, described above, are intended to allow companies track their supply and prove the provenance of products and also to assure consumers that the diamonds they are purchasing were mined by acceptable conditions.[95]

5.2.4 Risks and challenges

The issues underlying ethical and ecological sourcing tend to be sensitive and, in some cases, controversial. There is not always a consensus about the demands of "ethical" or "sustainable" production or whether certain practices aid or undermine the objective. Some of the stakeholders interviewed shared their experience of frictions with local NGOs.

In some cases, the commercial benefits of promoting sustainable practices may be too weak in some sectors to drive broader adoption of blockchain-based traceability systems.

Efforts by regulators to enforce standards will require a willingness of companies to join the blockchain network, and to cooperate in the development of the tracking system when the benefits to them are not sufficiently convincing. The failure of the pilot by the Dutch regulator to track rest times of lorry drivers illustrates the difficulties faced by public authorities.

5.3 Intellectual property protection

5.3.1 Current situation and problems

The emergence of new digital technologies and the rapid rise of the Internet have radically transformed the creative arts industry. Consumers now benefit from incomparably more options, while creators tackle the impact of the disruption on their ownership rights and compensation structures.[96] The music industry is the clearest example, and the focus of most blockchain initiatives within the creative industries.

After two decades of decline driven by access-based rather than ownership-based consumption, the 2017 music record industry revenues were 68% of those in 1999.[97] After the

[93] Coinsquare (2018). 'BMW Partners with Circulor to Bring Blockchain to Ethical Sourcing'. News article. 6 March 2018.
[94] Circulor Press Release (2018). 'Circulor blockchain brings real traceability to Tantalum mined in Rwanda'. Published 16 October 2018.
[95] ETH News (2018). 'Diamond Producer ALROSA Joins De Beers' Blockchain Pilot'. 30 October 2018.
[96] Rethink Music (2015). 'Fair Music: Transparency and Payment Flows in The Music Industry'. Rethink Music Initiative. A project of Berklee Institute of Creative Entrepreneurship.
[97] IFPI (2018). 'Global Music Report 2018: State of the Industry'.

initial piracy era of digital consumption, the era of legal downloads and streaming has slowed down and eventually reversed the fall of revenues in the music record industry.[98]

Of the $17 billion in global recorded music revenue, only a small portion beyond the initial recording advances makes its way to artists as ongoing revenue.[99] This is because the industry does not require streaming services and other intermediaries to provide complete, readable, up-to-date data about music sales and uses in an industry-standard format.[100] This means that artists often do not understand the royalty payments that they receive, with this opacity likely to benefit intermediaries.[101]

In addition, funds are often paid to wrong parties. Efforts to implement unique identifiers for sound recordings, such as the International Standard Recording Code (ISRC), are undermined by rights owners' persistence in defining their own standards for data reporting. Different services report in multiple formats, resulting in opacity and potential rights ambiguity. Large amounts of royalty revenue never reach the artist because owners cannot be accurately identified due to a lack of an industry-wide system for tying usage to ownership.[102]

5.3.2 Solutions offered by blockchain

Digital identities can be created for physical property and intangible assets, whose ownership and functioning can be controlled through smart contracts on the blockchain.

A report by the Blockchain For Creative Industries Research Cluster (BCI) at Middlesex University sees the potential of blockchain for the record industry in several areas:

- Blockchain technology could address the absence of a single database that documents ownership of all song and recording copyrights. Information stored on distributed ledgers rather than in silos would be updated instantly and automatically and made available to all users. The metadata embedded to recorded music could include the terms of use and contact details for the copyright holders, simplifying the identification of copyright owners and obtaining licences to use their work. Ultimately, the gradual placing of copyright data on the blockchain could result in one comprehensive copyright database for music.[103]
- Cryptocurrency transactions on the blockchain could also eliminate some intermediaries and boost the efficiency and transparency of royalty payments. The low transaction costs of cryptocurrencies (from the user's perspective) make it possible that content creators receive direct micropayments for music downloads or streaming and potentially even tips from consumers. Smart contracts could automate the administration of this process, including agreed splits between rights holders, bypassing intermediaries.[104] The transparency of copyrights and transactions recorded on public blockchains would help ensure that rights owners are identified, and royalties are paid to the correct party.[105]

---

[98] O'Dair et al (2016). 'Music on the Blockchain'. Blockchain For Creative Industries Research Cluster, Middlesex University, Report Nº 1.
[99] Rethink Music (2015).
[100] Rethink Music (2015).
[101] Rethink Music (2015).
[102] Rethink Music (2015).
[103] O'Dair et al (2016).
[104] O'Dair et al (2016).
[105] O'Dair et al (2016).

Applications of blockchain in the creative arts typically rely on public blockchain networks. This is because permissionless, public blockchains such as Bitcoin or Ethereum are the best option when absolute transparency is important, speed less so, and the application logic of the public protocol is sufficient for the objective at hand.

In addition, permissionless blockchains that are distributed across thousands of anonymous nodes protect the users of an application from its developers, who will not have control over any information stored on the ledger. Finally, public blockchains, to which anyone can contribute, benefit from being part of a large network. Adoption by a large number of content creators and rights owners is essential for ledger applications that aspire to create a comprehensive rights database for music or artworks.

5.3.3 Specific application(s)

Ujo Music

Empowering music

Mission

Ujo Music, a start-up backed by New York based blockchain software company ConsenSys, first came to public attention when it worked with musician Imogen Heap in 2015 to release her track "Tiny Human" on the Ethereum blockchain.

Using distributed ledger technology, the company is trying to build a transparent and decentralised database of rights and rights owners. This enables the use of royalty payments using smart contracts and cryptocurrency. Ujo's vision is to disintermediate the music industry, bridging the gap between musicians and listeners. Its platform aspires to give artists more control over their intellectual property by allowing them to gain more independence from major labels, and to easily track usage and payments for their work.[106]

Use of distributed ledger technologies

Ujo's key product is a database of music files connected to rights holders. Artists first register their identity in the 'Creator's Portal', a free mobile or desktop application. In the portal, they upload their work and specify licence conditions, including permitted use and price (for downloading, streaming, etc.).

The extent to which the software relies on distributed architecture is still evolving. At present, the platform logs the artist's identity on the public Ethereum blockchain. The blockchain also stores data linking the artist's identity to the uploaded music files, which are stored on off-chain online storage systems. When a consumer purchases the file, a smart contract on the blockchain is issued that logs the details of the payment, including the file identity, the beneficiary ID and the amount disbursed. The contract can also specify how the payment is divided between rights holders. Ujo itself – outside of the blockchain – then validates the payment. The company also performs the actual disbursement of the music file. Ujo therefore still relies on several centralised components but aspires for an entirely distributed infrastructure powered by crypto-economic incentives in the future.

[106] Ujo Music (2018a). "Introducing Ujo Portal: Making Musicians More Money", Blog published 13 December 2018.

Ujo hopes that the core layer of their platform, which includes the creator and licensee registry and payment channels, will become the bedrock for a broader ecosystem of decentralised applications connecting the musician and listener community. The platform should be interoperable with applications produced by other developers on top of the core, plugging into the underlying layer to provide new experiences including special events (e.g. concerts) or virtual interactions.

Progress to date

Until May 2018, Ujo Music was trialling its music registry on a test network. Since then, the Creator's Portal has run a publicly accessible beta test on the main Ethereum network. When the beta was launched, about 80 artists were on the platform.[107] As of early 2019, Ujo is running its first post-test version of the software. According to Ujo, this is the first-time artists are able to register their music directly on the main Ethereum blockchain and sell it for the network's cryptocurrency, Ether.[108]

Opportunities

Ujo Music is building a transparent and open music ecosystem for artists and supporters that is built on a secure and relatively accessible infrastructure. Its mission to give artists more control over their intellectual property may prove particularly valuable for early stage or less famous musicians, who struggle to monetise their work. By automating transactions in smart contracts, Ujo Music can also simplify the obtaining of usage rights, and the splitting of royalties between different parties.

Challenges

A key challenge for Ujo will be its ability to attract artists and consumers:

- Competing with streaming giants such as Spotify or YouTube, Ujo will need to demonstrate its value for listeners.
- The requirement for consumers to own and install specialised software may be an important obstacle.
- Many intermediaries in the music industry that Ujo plans to bypass may, in fact, add value (e.g. through payment negotiations, marketing, or paying advances to artists) and musicians may not find it advantageous to publish their work themselves.

5.3.3.1 Other notable examples

Other organisations and start-ups are also exploring the potential of blockchain technology for recorded music. **PeerTracks**, for example, is a streaming app built on blockchain, where listeners pay small royalties directly to artists every time they listen to a song. Unlike Ujo Music, which uses the volatile cryptocurrency Ether, PeerTracks uses a dual currency structure that exposes only the listeners to an exchange rate risk, while artists are compensated with a US dollar-pegged token. Other blockchain-based applications for recorded music include **Mycelia**, **Dot Blockchain Media**, **Bittunes** and **Aurovine**.

[107] Cheddar (2018). "Ujo Music Founder Says Blockchain Can Fix the Music Industry". Published 3 May 2018.
[108] Ujo Music (2018b). "The Ujo Platform: A Decentralized Music Ecosystem". Blog post. Published 3 July 2018.

5.3.4 Risks and challenges

Blockchain-based platforms for recorded music will face many challenges as they develop. Many are linked to the broader problems associated with permissionless public blockchains, such as scalability, speed, regulatory and legal uncertainty or environmental impact (see section 3.2.3). However, there are further issues directly connected to applications in the creative arts industry:

Fragmentation of the emerging ecosystem and a lack of interoperability between different platforms: While Ujo Music uses Ethereum, PeerTracks runs on the SOUNDAC blockchain and uses its own cryptocurrencies. Bittunes and Dot Blockchain Music rely on the bitcoin blockchain, while Aurovine uses yet another currency, its bespoke token Audiocoin.[109] The respondent from Ujo Music does not see this as a major problem, pointing out that that just like different countries have different currencies, different platforms can have different crypto currencies. This, however, assumes that exchanging between crypto currencies is as easy as exchanging US dollars for euros. In practice, different crypto tokens operating on different blockchains are not technologically compatible and cannot be easily exchanged.

Volatility of cryptocurrencies: The value of cryptocurrencies is often volatile and easily shaken by financial speculation. Most famously, the price of one Bitcoin fluctuated from $1,000 in January 2017 to $17,000 in December 2017 to just over $6,000 in November 2018.[110] Other cryptocurrencies including Ether followed a similar path. Such assets of unstable value are clearly impractical as a means of exchange in day-to-day payments.

Moreover, the ownership of cryptocurrencies requires specialised software and is still contained within a relatively small community. Cryptocurrency wallets, which require the management of private cryptographic keys, and other software tools needed for using blockchain networks, are perceived as opaque or untrustworthy. Outside the blockchain community, cryptocurrencies are not widely perceived as a credible alternative to fiat money (i.e. currency which has no intrinsic value but made legal tender by order of government). Instead, their reputation is still linked to illicit transactions and/or financial speculation.[111]

The music platforms will also need to develop a trustworthy governance system that ensures the integrity of the data. The obvious danger is that erroneous or fraudulent information is entered onto the immutable ledger. Corrections, also stored on the ledger, would be possible but it remains unclear who would verify the data or how disputes would be resolved.[112] It is also unclear whether blockchain technology can in fact prevent copying – even a microscopic edit of the same track would create a different cryptographic hash.[113] Platforms respond to these challenges by taking an active role in the verification of artists and restricting upload rights to such certified suppliers. However, such centralisation around the software operator raises the question whether the new platforms are actually that different from the intermediaries they seek to eliminate.

The platforms are likely to struggle to reach the critical mass that would lead to the creation of a comprehensive and authoritative database of music and rights. Earlier failed attempts such

---

[109] O'Dair et al. (2016) and websites of the individual platforms.
[110] CoinMarketCap
[111] UK Government Office for Science (2016).
[112] O'Dair et al (2016).
[113] O'Dair et al (2016).

as the Global Repertoire Database, the International Music Joint Venture or International Music Registry are often cited to illustrate the impossibility of the task.[114]

Finally, many in the industry may perceive blockchain technology as a threat rather than an opportunity and resist its adoption. These parties need not be limited to the record companies or publishers whose role the technology to some extent seeks to replace. Established artists signed with major record labels or artists who rely on advances received from the publishers may not find the economic model of cryptocurrency micropayments beneficial.[115]

5.4 Environmental control in pharmaceutical cold chains

5.4.1 Current situation and problems

The pharmaceuticals industry relies on longstanding supply chain and manufacturing paradigms and is generally cautious in adopting new technologies in operations.[116] However, the soaring complexity of supply chains, increasing competitive pressures, growing risk of counterfeit drugs, and rising regulatory scrutiny, pose considerable challenges to the industry. This has led to the need for more efficient supply chain management, greater transparency in the value chain and better-quality control.[117]

The processes in production and distribution of pharmaceuticals can have important consequences for the safety and quality of medicinal products. Pharmaceuticals can be diluted, counterfeited or substituted with lower quality products. The World Health Organisation (WHO) estimates that 1% of medicines available in developed countries are likely to be fraudulent. In the developing world, this figure surges to 10%, and in some parts of Asia, Africa and Latin America, fraudulent pharmaceuticals may comprise as much as 30% of the market.[118]

With the growing complexity and opacity of supply chains – which include suppliers of raw materials, manufacturers, logistics providers, wholesalers, distributors, pharmacies, and dispensing doctors – patient safety is increasingly becoming a principal concern for regulators. Both the US and the EU recently introduced legislation that requires an electronic system to trace and authenticate pharmaceutical products as they move through the supply chain network.[119]

Medicinal products could also be stored or transported in unsuitable conditions, such as incorrect temperature, humidity and/or excessive movement. Ensuring adequate environmental conditions (in particular, temperature) is an integral part of managing supply chains of perishable products such as vaccines or insulin. The total value of cold-chain logistics in the pharmaceutical sector has been estimated at $15 billion in 2018, growing 8% every year.[120] This compares with only 2% estimated growth for non-cold-chain logistics.[121]

---

[114] O'Dair et al (2016).
[115] O'Dair et al (2016).
[116] PwC (2016). 'Digitization in pharma: Gaining an edge in operations'. PwC Report. Published 19 October 2016.
[117] PwC (2016).
[118] WHO (2006). 'Counterfeit Medicines: an update on estimates 15 November 2006'. Updated 14 February 2018.
[119] Controlant (2018). 'When blockchain meets IoT and the food and pharmaceutical cold chains'. Blog post. 23 March 2018.
[120] Pharmaceutical Commerce (2018). 'The 2018 market for pharma cold chain logistics is $15 billion'. Article. Published 8 May 2018.
[121] Controlant (2018).

Businesses are under increasing regulatory pressure to provide evidence that shipped medicines and vaccines have not been exposed to conditions that could compromise their quality.[122] In the EU, distributors must comply with the European Commission guidelines on Good Distribution Practice (GDP 2013/C 343/01), effective since 1 January 2016. These regulations require proof that medicinal products for human use have been kept under suitable conditions.

The next section describes how blockchain technology can help the pharmaceutical sector improve efficiency and visibility of supply chains, ensure regulatory compliance, and protect consumers from falsified and mis-handled medicines.

5.4.2 Solutions offered by blockchain

Distributed ledger technology can be particularly useful in the pharmaceutical chains when combined with Internet-of-Things (IoT) sensors, radio-frequency identification (RFID) tags, and other technologies that allow real-time monitoring of individual products and environmental conditions in their surroundings. Combining blockchain with physical sensors and tags can enable downstream entities in the supply chain to monitor whether products have been kept at pre-agreed conditions. Transmitting and storing the sensor readings on a distributed ledger does not merely facilitate easy data sharing, but also ensures the integrity of the records. The data also provides a full, permanent and tamper-proof audit trail, supplying proof of compliance for regulators.

Sensor monitoring in the pharmaceutical cold chain also facilitates greater flexibility. Information transmitted by sensors provides real-time insights across the value chain that enable dynamic decisions in response to changing conditions.[123] This may reduce stockouts or help identify improper handling of medicines, ultimately saving lives. Moreover, many of these processes can be fully automated with the use of digital smart contracts.

In addition, the integration of blockchain with sensor technologies fosters accountability. Verifiable information about the product origin and specifications, environmental conditions throughout the distribution chain, and all transfers and transactions dramatically reduce ambiguity and increase accountability of individual participants in the supply chain. Smart contracts can provide automatic dispute resolution between business partners by, for example, triggering fines or ordering product recall when environmental conditions do not satisfy agreed rules.[124]

Monitoring medicines using sensor data stored on blockchain offers potential benefits to all stakeholders involved in the supply chain:

- Suppliers can obtain market advantage by offering real-time visibility into product handling and an authoritative audit log proving contract conditions have been fulfilled.[125]
- Retailers benefit from brand protection and a more efficient process for finding fault points and enforcing contractual penalties.[126]
- Regulatory bodies are better able to ensure safety using the information viewable on the shared ledger. The technology can help public authorities monitor compliance on a

[122] Controlant (2018).
[123] PwC (2016).
[124] Microsoft (2018a).
[125] Microsoft (2018a).
[126] Microsoft (2018a).

much larger scale, in real time, while at the same time reducing administrative costs (e.g. by automating inspections).

- Consumers benefit from increased confidence in the safety and quality of pharmaceuticals.

Specific applications of the blockchain technology in this case are examined in the following section.

5.4.3 Specific application(s)

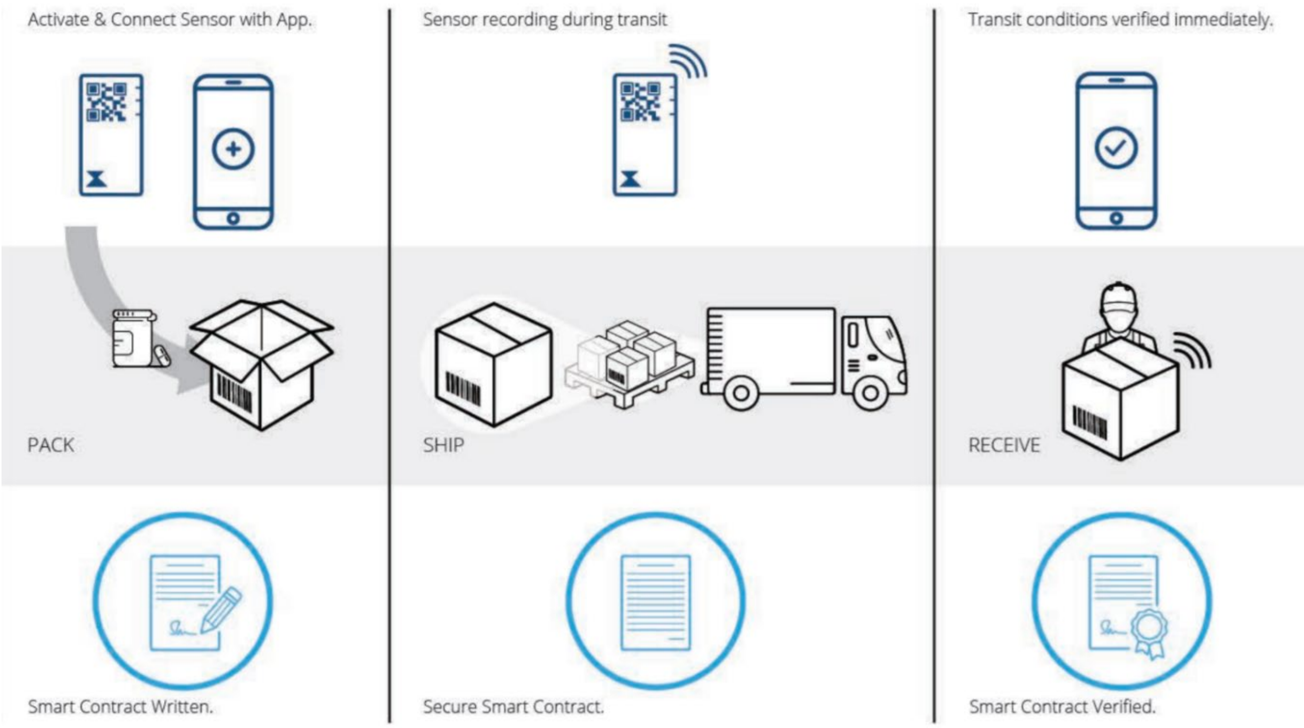
modum.io AG

Improving value chain automation in the pharmaceuticals industry

Mission

The distribution of medicinal products for human use is highly regulated, requiring the pharmaceutical industry to adopt increasingly complex processes for quality control and environmental monitoring.

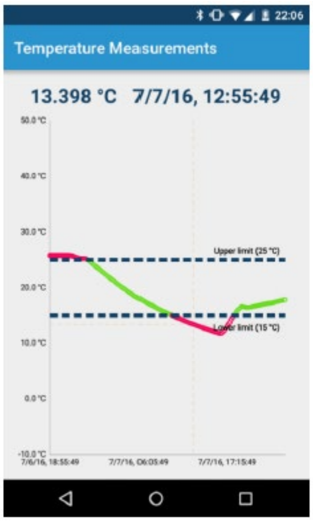
Modum.io, a Swiss start-up, was founded in 2016 to help distributors in pharmaceutical supply chains ensure regulatory compliance. The firm uses IoT sensor devices and blockchain technology to track pharmaceuticals that require temperature-controlled supply chains.



Use of distributed ledger technologies

Before a shipment occurs, a smart contract on the blockchain is written which specifies the ID of Modum's sensor device, shipment ID, and alarm criteria. While in transit, the temperature of each parcel is recorded by the sensor. When a change in ownership occurs, the collected data is transmitted to the blockchain and checked against the smart contract. The self-executing contract then validates that the transaction meets the standards set out by the sender, their clients, or the regulator and triggers various actions (approval, release of goods, release of funds, etc.). The distributed governance of the blockchain ensures that neither party can alter the collected temperature data or the terms of the contract.

Modum currently uses the public permissionless blockchain, Ethereum, but claims to be blockchain-agnostic and is already trialling the permissioned blockchain, Hyperledger Fabric, with some of its customers.



Progress to date

Modum completed three pilots in shipments from producer to wholesaler, wholesaler to clinics and pharmacies, and with a third-party logistics provider. It has since partnered with SAP and Swiss Post to integrate its solution with their track-and-trace systems, and in November 2018 launched its first commercially available solution, MODsense.

The company is also developing additional sensors, which would facilitate an expansion into the food and beverage, luxury goods, electronics, or medical supplies sectors.[127] A motion sensor, for example, can detect whether fragile goods have been handled appropriately, and a light sensor could detect whether the package has been opened during transit.

Opportunities

Modum claims that its system can substitute parts of the expensive, active temperature-controlled logistics services, and reduce the cost of proving regulatory compliance by as much as 60%.[128] The product is designed to provide an automated low-cost solution, easily integrated with existing systems and suitable for mass use, while at the same time offering a high level of data integrity, independent verification, auditability and security.

Challenges

The collected raw data could be manipulated prior to it being transmitted and verified against the smart contract criteria at the end of a transit stage. The sensor firmware might also be at risk of corruption. The risk is to some extent mitigated by several physical and digital security features implemented by Modum but cannot be eliminated entirely. Further potential vulnerabilities can arise from the blockchain technology itself.[129] For example, Modum's

[127] In September 2017, the firm raised $13 million in an Initial Coin Offering, the blockchain equivalent of a public listing on a stock exchange. Like ordinary shares, the MOD Token comes with voting and profit participation rights and is traded on several exchanges.
[128] Modum (2017). "White paper". Available at https://modum.io/sites/default/files/documents/2018-05/modum-whitepaper-v.-1.0.pdf. [Accessed on 06/11/2018]
[129] See section 2.2.3 for further details.

2016 pilot was affected by the DAO hack of Ethereum, which effectively disabled the smart contract used by Modum.[130]

5.4.3.1 Other notable examples

Some of the companies discussed in the context of food supply chains also plan an expansion to the pharmaceutical sector. **Ambrosus**, for example, is developing environmental loggers specifically targeted at pharmaceutical value chains.[131] These environmental loggers will collect data on temperature, humidity, pressure or sunlight exposure. Using wireless connectivity, the data will be logged on a blockchain network and should be accessible in real time through an app, enabling logistics providers to manage their cold chains more effectively.[132]

5.4.4 Risks and challenges

The pharmaceutical and life sciences industry sector is risk-averse and prefers to rely on established processes.[133] According to a source from Modum, implementation challenges can arise due to the difficulty of adding an additional step in a highly process-optimised industry.

Transparency may also face resistance from companies involved in the multi-billion-pound business with medicinal counterfeits and fraud. In addition, while electronically recorded and transmitted sensor data are more resistant to tampering than manual records, the hardware and software settings of the sensors may still be susceptible to fraud.

Several stakeholders suggested that it will still take considerable time before the full benefits of the technology are realised.

5.5 Food safety and standards

5.5.1 Current situation and problems

There are two main risks to the consumer that can originate from the food supply chain:

- Harm from food that is unsafe for human consumption (i.e. food safety).
- Misleading information about the product’s authenticity, composition or nutritional quality (i.e. food standards).

5.5.1.1 Food safety

Unsafe food is a global problem. According to the World Health Organization (2017), an estimated 600 million people fall ill every year after eating contaminated food, and 420,000 deaths are linked to foodborne diseases. Due to the complexity of modern food supply chains, it can take weeks or even months to identify and verify the source of an outbreak. Often, the cause is never found. In the 2015 outbreak of E. coli infections linked to the US restaurant chain Chipotle, an investigation led by the US Food and Drug Administration into Chipotle’s

[130] Bocek et al (2017). “Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain”. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM).
[131] Ambrosus (undated). “Pharmaceutical goods quality assurance and logistics”.
[132] Ambrosus (undated).
[133] PwC (2016).

upstream suppliers concluded that "*the distribution path did not lead to an ingredient of interest*" and "*no food item has been identified as causing the outbreak*".[134] In 2011, the estimated annual cost of foodborne illness in the United Kingdom was £1.84 billion.[135]

Food contamination can have various causes, some of which are directly related to supply chain processes or records. For example, a 2017 investigation discovered that the largest supplier of chicken to UK supermarkets altered the use-by date.[136]

Food may also be transported or stored in unsuitable conditions, for example, in too high temperatures. The absence of effective temperature-controlled supply chains – or cold chains – is a risk to consumer safety and a source of considerable supply chain inefficiencies and waste. In areas where cold chains are lacking, an estimated 200 million tonnes of food spoil before reaching the market every year.[137] Food may also get cross-contaminated by being stored or transported together with contaminated food.

5.5.1.2 Food standards

In other cases, food may be safe but of lower quality with different origin or containing different ingredients from those listed on the label. For example, in 2013, food inspections revealed that frozen beef burgers sold in several UK supermarkets contained up to 100% horsemeat.[138]

More common examples may involve misdescription of imported foodstuffs as 'locally produced', or conventionally cultivated crops as 'organic' to obtain premium prices. While food fraud is perceived to have a major significance, the level and impact of fraudulent or misleading practices is in most countries not documented systematically, and therefore almost impossible to quantify.[139] In the UK, the Food Fraud database documented 1,321 cases of food fraud in 2011. The consumer advocacy group, Which?, estimated the size of the UK counterfeit food market was £7 billion in 2008.[140]

While consumer safety and confidence are the most important objectives of food fraud prevention, businesses and public institutions can also be negatively impacted. The global financial impact of food fraud has been estimated at $40 billion each year.[141] [142] A single incident can permanently damage a brand, cause long-term industry-wide losses, close off export markets and damage trust in public authorities, inspectors and regulators.[143]

With longer and more complex supply chains, consumers are increasingly unaware of how their food is produced but even retailers and wholesalers may not have an overview of the entire product chain. Against this backdrop, consumers are demanding trustworthy and verifiable information about the origin of foodstuffs, including whether a food product is sourced

---

134 US Food & Drug Administration (2016). 'FDA Investigates Multistate Outbreak of E. coli O26 Infections Linked to Chipotle Mexican Grill Restaurants'. Report. 1 February 2016.
135 Food Standards Agency (2011), cited in National Audit Office (2014). 'Food safety and authenticity in the processed meat supply chain'. Report by the Comptroller and Auditor General.
136 The Guardian (2017). 'UK's top supplier of supermarket chicken fiddles food safety dates'. Article. Published 28 September 2017.
137 Roberson (2015). 'Innovation in global cold chain transport is helping to reduce food and medical waste'. TradeReady Blog. Published 17 September 2015.
138 BBC (2013). 'Q&A: Horsemeat scandal'. Published 5 February 2013.
139 Dennis and Kelly (2013).
140 Dennis and Kelly (2013).
141 Spink, J. (2014), cited in PwC (2015). 'Food Fraud Vulnerability Assessment and Mitigation'.
142 This figure is not directly comparable with the £7 billion estimate for the UK. Quantitative estimates of the impact of food fraud are notoriously difficult given the absence of official data. Moreover, the methodologies can differ substantially, for example in their assumptions about the indirect impact of food fraud.
143 PwC (2015). 'Food Fraud Vulnerability Assessment and Mitigation. Report 2015.

in a certain way.[144] Locally produced or organic are just two examples; others may include vegan, fair trade, free range, non-GMO or halal/kosher.

5.5.2 Solutions offered by blockchain

Distributed ledger technology can facilitate a more efficient and trustworthy system of tracing foodstuffs along the supply chain.

Blockchain-powered software solutions can give farmers, aggregators, processors, transporters, wholesalers, retailers, and potentially also governments/authorities and consumers a secure, shared view of the full food supply chain. As the product moves downstream from farm to store, participants in the network add time-stamped transactions to the ledger whenever the product changes hands. The data could also include various product, environmental, and quality specifications. Each added transaction is encrypted and validated through a consensus by the participating network nodes, with the precise mechanism determined by the blockchain protocol.[145] If validated, the new block is added to the blockchain and the ledger itself is simultaneously updated on all computers, which hold identical copies. The unique, but distributed source of truth thus stores the full product history which cannot be unilaterally modified by any individual entity.

Attestable food provenance could help prevent food contamination as well as food fraud. By limiting the possibility to tamper with safety records and eliminating incentives to produce or handle food inappropriately, supply chain transparency could decrease the number of unsafe products in the market. The ability to track the source of a contamination outbreak would also help in containing its spread and in identifying the accountable parties. Similarly, tamper-proof authenticity certificates would make it much harder to commit food fraud.

Traceability of food products could bring benefits to all involved parties:

- Suppliers may obtain market advantage from public recognition for certifiable sourcing practices.
- Retailers face lower risk of selling unsafe or inauthentic products, and their ability to prove product provenance can help them boost brand loyalty.[146]
- Regulators are better able to stop unsafe or fraudulent products from entering the market, trace the source of a contamination outbreak, prevent cross-contamination, and sanction accountable parties.
- Consumers benefit from lower health risks and higher confidence in products. Improved traceability also allows consumers to better distinguish between brands based on alignment with values.[147]

As of early 2019, most identified blockchain solutions for food traceability are currently in the stage of proofs of concept, prototypes or pilots. However, even if the experiments convince businesses that blockchain-based food traceability systems are a viable long-term investment, the same industry conservatism that is also found in the pharmaceuticals sectors means that it

[144] Provenance (2015). 'White Paper'.
[145] See section 2.2.1 for further details.
[146] Microsoft (2018a).
[147] Microsoft (2018a).

may still take several years before they achieve wider commercialisation and mass market reach.

A broader adoption may also depend on overcoming the scalability problems of permissionless blockchains. Some of the avenues currently explored rely, for example, on faster permissioned blockchains or hybrid structures.[148]

5.5.3 Specific application(s)

IBM®

IBM Food Trust

Tracking food supply chains with a trusted, shared and immutable ledger

Mission

An early mover in the blockchain-as-a-service (BaaS) industry, IBM provides one of the pioneering technological solutions for food traceability. In collaboration with major players in the agri-food market – Walmart, Nestle, and Dole among others[149] – IBM Food Trust™ aims to increase transparency and trust in global food supply by connecting food producers, suppliers, distributors, and retailers in a permissioned blockchain network that traces food products from farm to store, and eventually to consumers.

Use of distributed ledger technologies

Participants along the value chain upload their supply chain data to a shared ledger, creating encrypted tamper-resistant records that can be shared with business partners. The IBM blockchain solution, based on open-sourced Hyperledger Fabric, facilitates a permission-based, shared view of the food ecosystem, allowing participants to enter and control shared access to their blockchain data. [150]

If a food safety issue arises, participating organisations can quickly locate affected items from the supply chain by querying product identifiers. If the organisation is permissioned to see the data, the result is immediate access to the complete history and current status of the food item along with accompanying information such as certifications or test data. [151] [152]

Progress to date

Several high-profile players in the food sector are using IBM's software for their traceability programmes. Europe's largest retailer, Carrefour, announced in March 2018 that it will roll out its IBM-powered traceability system to eight more products after a successful test with Auvergne chickens. The retail chain expects to expand the programme to all Carrefour brands by 2022. [153] [154] In September 2018, Walmart announced their blockchain-enabled Traceability Initiative and issued a letter to its direct suppliers of leafy greens requiring that

[148] See, for example, IBM Food and TE-FOOD case studies.
[149] Supermarket News (2018). "More retailers join IBM Food Trust network".
[150] IBM Food Trust Solution Brief 2.0 (2018).
[151] IBM Food Trust Solution Brief 2.0 (2018).
[152] IBM Food Trust Solution Brief 2.0 (2018).
[153] Carrefour (2018). "Press Release". 6 March 2018.
[154] Carrefour (2018).

they capture traceability data using IBM Food Trust.[155] By September 2019, Walmart expects to have end-to-end traceability across their leafy green supply chain.

After 18 months of testing, IBM Food Trust matured to the production stage in October 2018. A range of supply chain partners is already sharing data on the blockchain platform. However, according to a source from IBM Food Trust, given the length and complexity of supply chains in the global food sector, the initiative has only scratched the surface on the potential for value in the food supply chain.

Opportunities

According to IBM, the Food Trust ecosystem could mitigate the spread of food-borne illnesses, cross-contamination and waste. It could also certify provenance and ensure food quality and authenticity, increase efficiency, and reduce product loss.[156]

Direct insight into the full supply chain could help companies identify and address inefficiencies and increase consumer satisfaction and trust. During a foodborne outbreak, the company can prove that its product is safe or trace contaminated foods, enabling it to act much more quickly.

Challenges

The ability to trace food products end-to-end within the IBM Food Trust ecosystem crucially depends on data availability. All participants in the value chain must upload their data and choose what data they share with whom. According to a source at IBM Food Trust, creating an ecosystem that provides value for all participants, and agreeing to the rules of collaboration, are focus areas for IBM as the initiative scales globally.

Moreover, full traceability may require companies to engage in costly investment in new procedures, processes, jobs or training. This concern is particularly salient given the potentially unequal distribution of costs and benefits along the food supply chain. While many of the additional costs of data collection (or digitisation) are likely to be borne by farms and suppliers at the beginning of the supply chain, companies at the end of the chain (wholesaler and retailers) are likely to benefit the most from full traceability.[157] Although all engaged parties are likely to benefit from full traceability, the value will be different for various stakeholders. According to the source at IBM Food Trust, it is important to ensure that the value received is proportional to the investment being made.

Other large technology companies are also active in the development of blockchain-based services for food traceability.

- **Intel** built a prototype using their own blockchain protocol, which combines a distributed ledger and IoT sensors to track key parameters throughout the capture, processing and transit of fish.[158]

[155] Walmart (2018).
[156] IBM Food Trust Solution Brief 2.0 (2018).
[157] TE-FOOD (2017c). ‘Challenges of a food traceability system implementation’. Blog post on Medium. 10 November 2017.
[158] Sawtooth (undated). ‘Bringing traceability and accountability to the supply chain through the power of Hyperledger Sawtooth’s distributed ledger technology’.

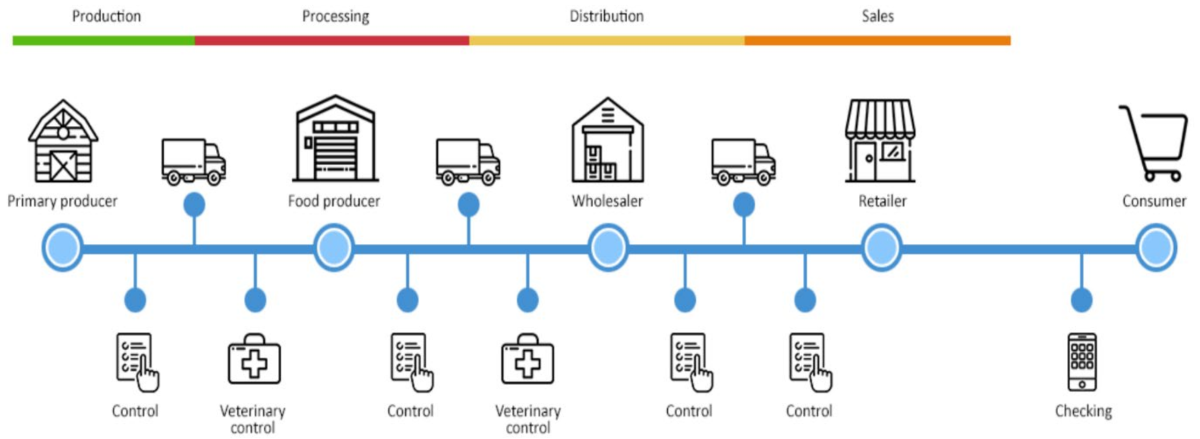
- **Microsoft** added blockchain to its cloud software solutions and recently partnered with the grain processing giant Bühler to track grain and maize as it moves across the supply chain.[159]

TE-FOOD

Farm-to-table fresh food traceability for emerging markets

Mission

Unlike other blockchain-based product tracking start-ups, a Vietnamese-Hungarian company TE-FOOD, founded in 2015, already provides an established, commercially available solution for tracing the production and distribution chains of pigs, chickens and eggs in Vietnam. The firm's current ambition is to transition to a blockchain-based infrastructure that would increase the credibility and transparency of the stored data by distributing access and control. A blockchain architecture also unlocks new funding opportunities for a planned expansion into other markets and products.



Use of distributed ledger technologies

The existing tracking system is implemented physically through product identification tags and security seals and digitally through B2B and consumer apps. Throughout the supply chain the product information is (often manually) recorded in B2B mobile apps where it can also be accessed by food safety authorities and other regulators. The system is used by 6,000 businesses including farms, livestock agents, slaughterhouses, food producers, veterinary companies, wholesale distributors and retailers[160].

Using QR codes on product labels, the information with product origin and full history is available to over 30 million consumers, 50,000 of whom have downloaded the consumer app[161]. Until recently, the collected data was stored and centrally managed by TE-FOOD.

[159] Microsoft (2018b). 'Bühler will track crops from farm to fork using blockchain technology'. Microsoft Industry Blogs. Published 25 September 2018.
[160] TE-FOOD (2017a). 'White paper'.
[161] TE-FOOD (2017b). 'TE-FOOD – Modum comparison'. Blog post on Medium. 18 December 2017.

TE-FOOD's new architecture relies on two blockchains and will operate as follows:

- TE-FOOD raises funds by selling crypto tokens (TFD) on the Ethereum platform. The tokens act primarily as "software licenses" for those who wish to verify transactions on TE-FOOD's own permissioned blockchain (FoodChain).[162]
- FoodChain records and stores the actual traceability data and uses a different, USD-pegged token (CAL) as currency to pay for various services within the TE-FOOD ecosystem:
- Holders of the software licence provide computation power to validate and store transactions. They are compensated with newly minted CAL.
- Food supply chain companies must buy CAL to log data in the traceability app. CAL is burned through use.

The crypto-economic design envisioned by TE-FOOD therefore relies on a version of mining.[163] Users of the traceability system pay the distributed service providers for maintaining the ledger. Unlike other cryptocurrencies, however, the underlying token is pegged to the US dollar and not freely traded, and so cannot therefore be used for financial speculation.

Progress to date

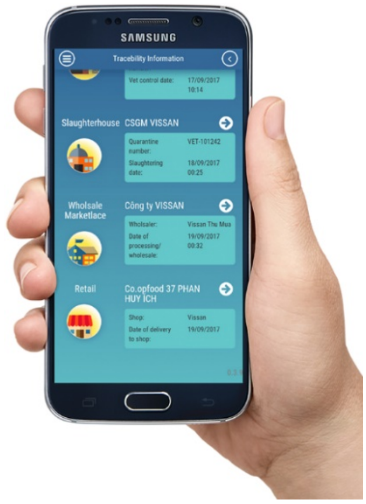
As of early 2019, TE-FOOD's operations have been migrated to FoodChain.

Opportunities

[162] The sale took place in February 2018. The combined funds raised from the private and public sale amounted to USD 19 million. 'TE-FOOD, Token Release Update', https://medium.com/@te_food/token-release-update-5365a4c3d83d

[163] See section 2.2.2. The implementation chosen by TE-FOOD resembles a Proof-of-Stake consensus algorithm.

By distributing access and control of the ledger, TE-FOOD hopes to strengthen trust and engagement in its traceability system. Using the raised funds, the firm also aspires to extend its operations to include more emerging markets, new technologies (including food safety sensors and animal face recognition tools), and other products including cattle, fruits, vegetables, arable crops, fish, and seafood.



Challenges

TE-FOOD's transition to blockchain does have a number of risks linked to the complicated and unconventional governance mechanisms and crypto-economic incentives of its blockchain infrastructure. It is also possible that some regulators could see TE-FOOD's cryptocurrency as being a security, which could lead to restrictions on the firm's operations.

Experiments by public authorities of using blockchain to ensure regulatory compliance in the food sector are rare. In July 2018, the **UK Food Standards Agency** (FSA) announced it had completed a pilot using blockchain technology in a cattle slaughterhouse, and more recently, launched a second pilot to track health certification information for pork exported to China.

Using a permissioned private blockchain in its first pilot, the FSA collected and shared information on cattle carcass inspections to improve traceability and address data quality issues in the provenance of red meat. Periodically, farmers recorded key information about an animal (such as their weight and disease applications) onto the Farm2Fork application, which was uploaded onto the blockchain ledger. Once the animal had reached a specific age and weight, food business operators (FBOs) had the option to purchase them for a negotiated price. At the abattoir, FSA official veterinary and meat inspectors recorded information on anti- and post-mortem conditions of the cattle using unique animal ear-tags onto the blockchain ledger.

The use of blockchain in this instance allowed the FSA to run detailed condition reports by FBO, site and animal, which were previously unavailable. FBOs were also able to view the reported condition for any animals placed on their farm. The FSA noted that the use of blockchain provided efficiency gains from reduced duplication and reduced burden of data entry and is planning to undertake an evaluation to see whether these gains translated into cost savings.

TE-FOOD already shares its data with veterinary authorities. The company also designed a system of food safety alerts – triggered by events such as livestock transport taking longer than average – that automatically notify the competent authority.[164]

5.5.3.1 Other notable examples

The technological and commercial opportunities offered by blockchain have also led to the creation of numerous technology start-ups focusing on tracking food products. A London-based start-up **Provenance**, for example, partnered with a local non-profit organisation in 2016 to pilot blockchain technology for tracing yellowfin and skipjack tuna fish in Indonesia from

[164] TE-FOOD (2017a).

catch to consumer.[165] Unlike the permissioned blockchain implementations offered by large tech companies, Provenance traces food items using a decentralised application running on the public blockchain Ethereum.[166] Businesses along the supply chain log information about the food item in the app, while a system of tags links the physical products with their digital identity. Provenance claims to work with over 200 retailers and producers in the food industry, including The Co-operative supermarket chain.[167] However, the speed limitations of public blockchains[168] present a major obstacle to wide commercialisation. According to Provenance's founder and CEO Jessi Baker, public blockchains "have a long way to go before they can be applied at scale".[169]

Some start-ups are offering integrated blockchain-based hardware and software products for farm-to-store food traceability. Swiss-based **Ambrosus** is developing a system that utilises sensors and biosensors to track and transmit in real-time a product's physical attributes and its surroundings, using electronic ID-tagging and anti-tampering mechanisms. The sensor data are transmitted and stored on AMB-NET, a personalised Ethereum-compatible blockchain protocol with encoded smart contracts, which can automatically resolve quality, safety, or logistical disputes between supply chain participants.[170]

Ambrosus recently partnered with NDS, a subsidiary of Korean food producer Nongshim, for a proof-of-concept to track and trace beef sold by food retailer Mega Mart.[171] Ambrosus will develop IoT sensors, which will transmit readings including the location, quality, and temperature of the beef directly to AMB-NET.[172] The immutably stored data on the blockchain can then be configured for example in the form of a consumer application. According to the Co-Founder and CEO Angel Versetti, "through a QR code, the specific cow, its origin, the veterinarian's health check of the meat, and the transportation conditions of the product will all be easily accessible to the consumer through the scan of a smartphone".[173] Other companies, such as China-based start-up, **Waltonchain**, are developing their own electronic tags and patented IoT devices to track the provenance of foodstuffs.

Other start-ups focus on helping businesses attest authenticity of frequently counterfeited food items. Edinburgh-based **Arc-net** partnered with the whisky producer Adelphi to track each bottle of the spirit through the manufacturing and distilling process. According to arc-net, consumers of Adelphi's whisky will be able to access the data and verify the authenticity of the product.[174]

5.5.4 Risks and challenges

A broader market adoption of systems tracking food supply faces several challenges.

---

165 Provenance (2016). 'From shore to plate: Tracking tuna on the blockchain'.
166 Provenance (2015). "White Paper".
167 Provenance website. Available at https://www.provenance.org/case-studies [Accessed 31/10/2018]
168 See section 2.2.3 for further details.
169 Cited in The Guardian (2018), 'Does blockchain offer hype or hope?' 10 March 2018. Available at https://www.theguardian.com/technology/2018/mar/10/blockchain-music-imogen-heap-provenance-finance-voting-amir-taaki [Accessed 31/10/2018]
170 Ambrosus website. Available at https://ambrosus.com/#technology [Accessed 01/11/2018]
171 Food, Drink & Franchise (2018). 'Could blockchain and IoT enhance food safety? Q&A with Ambrosus Co-founder & CEO Angel Versetti'. Published 31 October 2018.
172 Food, Drink & Franchise (2018).
173 Food, Drink & Franchise (2018).
174 Arc-net (2017). 'World First - arc-net and Adelphi's Ardnamurchan Distillery partner to put the first Scottish Spirit and Whisky on arc-net's Blockchain platform'. Press release. 27 September 2017.

- The agri-food supply chain is a well-established industry, typically characterised by small margins. Businesses may be sceptical of embryonic technologies or unwilling to invest in potentially costly hardware and software, introduce new procedures, train workers, or redesign carefully optimised processes.

- Competition will restrict the ability of the supply chain to pass the costs on to consumers. This concern is particularly salient given that many of the costs of blockchain-based traceability systems are likely to be borne by farms and suppliers at the beginning of the supply chain, while companies at the end of the chain (retailers) are likely to benefit the most.[175]

- Widespread adoption might be slowed down by those who benefit from poor traceability. Counterfeiting, food fraud and inadequate standards constitute a loss to society but a source of income for the responsible parties. However, a frequently expressed view among stakeholders was that this obstacle is unlikely to cause major problems in the long run as the increasing demand for transparency from consumers and downstream businesses in supply chains will drive the adoption of full traceability.

- Applications of blockchain in more traditional and risk-averse industries may also suffer from negative connotations associated with cryptocurrencies, often seen as a speculative bubble or a vehicle for trade with illicit goods. Many blockchain food traceability systems, however, do not rely on cryptocurrencies at all (e.g. IBM Food Trust).

- Blockchain technology cannot prevent all risks associated with data integrity. Where data are manually entered into the ledger they can be adulterated already at input. Moreover, the subsequent resistance of the ledger to tampering relies on the specific protocol, cryptography and governance structure of the blockchain[176]. Permissioned blockchains, for example, can use a consensus mechanism where one or two dominant network participants can modify the data entries.

[175] TE-FOOD (2017c). 'Challenges of a food traceability system implementation'. Blog post on Medium. 10 November 2017.
[176] See section 2.2.3 for further details.

This publication is available from: www.gov.uk/beis

If you need a version of this document in a more accessible format, please email enquiries@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.